European Commission

LEGAL ASPECTS OF MARITIME MONITORING & SURVEILLANCE DATA

Framework Service Contract, No. FISH/2006/09 – LOT2

Final Report

submitted to:

DG Maritime Affairs & Fisheries

by

MRAG

in association with

BIRD & BIRD

October 2008
### 3.6.5 Who has a right to the data?

### 3.7 Port Security Notification Requirements – Regulation 725/2004 (EC)
- **3.7.1 Background and legal basis**
- **3.7.2 What data is reported?**
- **3.7.3 Why is the data reported?**
- **3.7.4 Who has a right to the data?**

### 3.8 Schengen notification requirements
- **3.8.1 Background and legal basis**
- **3.8.2 What data is reported?**
- **3.8.3 Why is the data reported?**
- **3.8.4 Who has a right to the data?**

### 4 Surveillance systems

#### 4.1 Military surveillance systems
- **4.1.1 Background and legal basis**
- **4.1.2 What data is collected?**
- **4.1.3 Why is the data collected?**
- **4.1.4 Who has a right to the data?**

#### 4.2 SIVE
- **4.2.1 Background**
- **4.2.2 Legal basis**
- **4.2.3 What data is collected?**
- **4.2.4 Why is the data collected?**
- **4.2.5 Who has a right to the data?**
- **4.2.6 Data sharing in practice**

#### 4.3 Vessel Traffic Services (VTS)
- **4.3.1 Background**
- **4.3.2 Legal basis**
- **4.3.3 What data is collected?**
- **4.3.4 Why is the data collected?**
- **4.3.5 Who has a right to the data?**

#### 4.4 CleanSeaNet
- **4.4.1 Background and legal basis**
- **4.4.2 What data is gathered?**
- **4.4.3 Why is the data gathered?**
- **4.4.4 Who has a right to the data?**

### 5 Data sharing mechanisms

#### 5.1 National data sharing mechanisms
- **5.1.1 France**
- **5.1.2 Finland**

#### 5.2 Regional AIS data sharing agreements
- **5.2.1 HELCOM AIS Network**
- **5.2.2 Other regional AIS Networks**

#### 5.3 SafeSeaNet
- **5.3.1 Background and legal basis**
- **5.3.2 What data is shared?**
- **5.3.3 Who has a right to the data?**

#### 5.4 Commercial AIS data sharing mechanisms
- **5.4.1 Background and legal basis**
<table>
<thead>
<tr>
<th>Annex A</th>
<th>Terms of Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex B</td>
<td>List of instruments consulted</td>
</tr>
<tr>
<td>Annex C</td>
<td>Excerpt from the German Federal Maritime Responsibilities Act</td>
</tr>
<tr>
<td>Annex D</td>
<td>Summary of findings</td>
</tr>
</tbody>
</table>
### Acronyms and abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>Automatic Identification System</td>
</tr>
<tr>
<td>AIS Guidelines</td>
<td><em>Guidelines for the onboard operational use of ship-borne Automatic Identification Systems (AIS)</em> adopted by the IMO by Resolution A.917 (22)</td>
</tr>
<tr>
<td>Article 29 WP</td>
<td>Working Party on the Protection of Individuals with regard to the Processing of Personal Data</td>
</tr>
<tr>
<td>BRITE</td>
<td>Baseline for Rapid Interative Transformational Experimentation</td>
</tr>
<tr>
<td>CALDOVEREP</td>
<td>Calais-Dover Reporting System</td>
</tr>
<tr>
<td>CFP</td>
<td>Common Fisheries Policy</td>
</tr>
<tr>
<td>CFR</td>
<td>Community Fleet Register</td>
</tr>
<tr>
<td>COLREGS</td>
<td>Convention on the International Regulations for Preventing Collisions at Sea, 1972</td>
</tr>
<tr>
<td>Control Regulation</td>
<td>Regulation (EEC) No 2847/93 establishing a control system applicable to the common fisheries policy</td>
</tr>
<tr>
<td>CROSS</td>
<td><em>Centres Régionaux Opérationnels de Surveillance et de Sauvetage</em> (France)</td>
</tr>
<tr>
<td>Data Protection Directive</td>
<td>Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data</td>
</tr>
<tr>
<td>Data Protection Regulation</td>
<td>Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data</td>
</tr>
<tr>
<td>DEFRA</td>
<td>Department of Environment, Fisheries &amp; Rural Affairs (UK ministry)</td>
</tr>
<tr>
<td>DMA</td>
<td>Directorate of Maritime Affairs (France)</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EEZ</td>
<td>Exclusive Economic Zone</td>
</tr>
<tr>
<td>EIS</td>
<td>European Index Server</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EC</td>
<td>European Community</td>
</tr>
<tr>
<td>EMSA</td>
<td>European Maritime Safety Agency</td>
</tr>
<tr>
<td>EU LRIT DC</td>
<td>proposed European Union LRIT Data Centre</td>
</tr>
<tr>
<td>EUROSUR</td>
<td>European Border Surveillance System</td>
</tr>
<tr>
<td>EUROSUR Communication</td>
<td>Communication from the Commission to the European Parliament, the Council, the European Economic and Social</td>
</tr>
</tbody>
</table>
Committee and the Committee of the Regions examining the creation of a European Border Surveillance System

**FAL Convention**  
Convention on Facilitation of International Maritime Traffic (IMO)

**FMC**  
Fisheries Monitoring Centre

**Framework Regulation**  
Council Regulation (EC) No 2371/2002 of 20 December 2002 on the conservation and sustainable exploitation of fisheries resources under the Common Fisheries Policy

**GNSS**  
Global Navigation Satellite System

**GOFREP**  
Gulf of Finland Reporting System

**GPS**  
global positioning system

**HELCOM**  
Helsinki Commission

**IBC**  
International Code for the Construction and Equipment of Ships Carrying Dangerous Chemicals in Bulk

**IGC**  
International Gas Carriers’ Code

**IMDG**  
International Maritime Dangerous Goods Code

**IMO**  
International Maritime Organisation

**ISO**  
International Standards Organisation

**ISPS Code**  
International Ship and Port Facility Security Code

**IT**  
information technology

**ITU**  
International Telecommunications Union

**LCA**  
Local Competent Authorities

**LRF**  
Lloyds Register-Fairplay Limited

**LOS C**  

**LRIT**  
Long-Range Identification and Tracking of Ships

**MAOC-N**  
Maritime Analysis & Operations Centre - Narcotics

**MARPOL**  
International Convention for the Prevention of Pollution from Ships, 1973 as amended

**MCA**  
Maritime & Coastguard Agency (UK)

**MCCIS**  
Maritime Command and Control Information System

**MID**  
Maritime Identification Digits

**MMSI**  
Maritime Mobile Service Identity

**MoU**  
memorandum of understanding

**MRCC**  
Marine Rescue Coordination Centre

**MSA**  
Maritime Situational Awareness

**MSC**  
Maritime Safety Committee (of the IMO)

**MSSIS**  
Maritime Safety and Security Information System

**NATO**  
North Atlantic Treaty Organisation

**nm**  
nautical mile

**OOW**  
officer of the watch

**PNR**  
Passenger Name Record

**Port Security Regulation**  

**PSI Directive**  
Directive 2003/98/EC on the re-use of public sector information of 17 November 2003

**SAR**  
search and rescue

**SAR Convention**  
International Convention on Maritime Search and Rescue 1979 (as amended)

**SAM**  
situation d’approches maritimes (France)

SIVE Sistema Integrado de Vigilancia Exterior (Spain)

SOLAS International Convention for the Safety of Life at Sea, 1974

SOTDMA self organising time division multiple access

STIRES SafeSeaNet Traffic Information Relay and Exchange System

Transparency Regulation Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents

UK United Kingdom

UTC coordinated universal time

VHF very high frequency

V-RMTC Virtual Maritime Traffic Centre

VMS vessel monitoring system


VTS Vessel Traffic Service

WETREP Western European Tanker Reporting System
1 Introduction

1. Maritime monitoring and surveillance data is currently gathered within and around European waters by a range of agencies for a number of different purposes including fisheries management, the promotion of safe navigation, policing the seas and border and immigration control. At the same time various different mechanisms exist for the exchange of military surveillance data gathered by European navies.

2. In itself this is not something new: the monitoring and surveillance of activities in the waters off Europe’s coasts has taken place for many hundreds of years and the routine exchange of naval surveillance data is well established.

3. Of course the focus and scope of maritime monitoring and surveillance has changed with the passage of time: the rum smugglers of old have been replaced with the smugglers of narcotics and traffickers of people. In recent years illegal immigration by sea has become a major issue particularly along Europe’s southern borders. The enormous growth in maritime traffic in Europe’s waters has been accompanied by increased monitoring and surveillance designed to ensure the safety of navigation and the prevention of maritime pollution. Changes in international law in the 1970s have seen a major increase in the scope of monitoring and surveillance of fisheries activities by Europe’s coastal States.

4. As regards naval surveillance a combination of the end of the ‘cold war’ and the terrorist attack on New York on 11 September 2001 has seen Europe’s navies shift their surveillance focus away from the ‘grey’ military ships of the former Warsaw Pact to ‘white’ civilian ships that may be used in connection with terrorism.

5. Changes in the focus and scope of maritime monitoring and surveillance have of course been accompanied by changes in the technology used: from telescopes and binoculars through to radar and the satellite and computer based surveillance techniques used today.

6. The focus of this Study is on one aspect of these technological developments namely the ability of States and state agencies to remotely acquire large amounts of ‘real time’ or near ‘real time’ maritime monitoring and surveillance data and to process and share that data, also in real time or near real time, through the use of computers and modern telecommunications methods including the internet. More particularly the Study seeks to provide a better understanding of the legal rights and restrictions that apply to the use and sharing of maritime monitoring and surveillance data relating to vessels, individuals and activities gathered through a range of existing systems such that could be combined into a common European information sharing environment for the marine domain. A copy of the terms of reference is attached as Annex A.¹

7. The background to this Study is the ongoing development of a Maritime Policy for the European Union (EU). The year-long public consultation exercise for the

¹ The terms of reference in fact refer to two separate studies contained in the same work package. The terms of reference relating to the present Study are those relating to task one.
Maritime Policy revealed broad stakeholder support for further integration of maritime monitoring and surveillance data.

8. On 10 October 2007 the European Commission adopted a Communication\(^2\) setting out its vision for an Integrated Maritime Policy for the EU, together with a detailed action plan\(^3\) setting out a work programme for the years ahead. This vision was welcomed by the European Council of 14 December 2007 and the Commission was invited to come forward with the initiatives and proposals contained in the action plan.

9. As provided for in the action plan, the Commission is due to adopt in the second half of 2008 a Communication that will contain a work plan for further steps towards the integration of all European maritime reporting and surveillance systems. This will go beyond border related aspects, thus covering all maritime activities, such as maritime safety, protection of the marine environment, fisheries control, and law enforcement. This Study seeks to contribute to a better of understanding of the legal issues relating to the collection, use and sharing of ‘real time’ surveillance data that will feed into the planned Communication. In particular the Study seeks to identify what legal obstacles exist to the sharing of maritime data between public authorities in the Member States and thus the envisaged integration mechanism.

10. More specifically, the basic questions that are examined in this Study are: (a) What data are collected/used/shared? (b) What is the legal basis for this? (c) Why is the data collected/shared? (d) Who is entitled to the data? (e) What are the legal restrictions, if any, on sharing the data between public agencies?\(^4\)

11. Although the focus of this Study is on the area of law known as ‘data law’\(^5\) maritime monitoring and surveillance activities take place against the background of the sea and the Law of the Sea. The Law of the Sea, is the branch of (public) international law\(^6\) that regulates the rights and duties of states and other actors recognised by international law, such as the European Community, concerning the sea and marine. Part Two therefore contains a brief description of the elements of the Law of Sea that are relevant to this Study.

12. Careful analysis shows that the Study terms of reference are in fact concerned with what are essentially three different types of mechanism. For the purpose of analysis these can be broken down as follows:

- (a) ‘reporting regimes’;
- (b) ‘surveillance schemes’; and
- (c) ‘data sharing mechanisms’.

\(^4\) In addition, in cases where such practices were determined, examples of data-sharing are provided.
\(^5\) Data law includes everything that has to do with information including data protection. Data law is often seen as a sub-set of information technology (IT) law but the scope of IT law which includes electronic commerce, the internet, software contracts, outsourcing and computer crime is far broader.
\(^6\) As opposed to ‘private’ international law, sometimes known as the ‘conflict of laws’, which is concerned with determining the applicable law in trans-jurisdictional disputes.
13. For the purpose of discussion these three types of mechanism will be referred generically as ‘schemes’. In fact the situation is a little more complex because, as will be seen, some schemes (such as VTS) make use of data that is both actively reported (pursuant to a reporting regime) as well as to surveillance data (from a surveillance scheme).

14. Under the heading ‘reporting regimes’ are included those regimes whereby data must be actively reported by a person or vessel subject to the applicable regime. The reporting requirement may be automated or manual or both. These regimes are examined in Part Three.

15. Under the heading ‘surveillance schemes’ can be included arrangements under which data is gathered by surveillance methods in respect of which the person who is subject to the scheme plays no active part. These schemes are examined Part Four. Part Five contains a description of various existing data sharing mechanisms.

16. Part Six contains a detailed analysis of the potential legal barriers to the exchange of maritime monitoring and surveillance data while conclusions are drawn in Part Seven.
2 The Law of the Sea

17. The sources of the Law of the Sea include customary international law as well as a range of multilateral and bilateral treaties and regulations adopted under them.

18. The most important of these instruments is the United Nations Convention on the Law of the Sea (LOS) adopted at Montego Bay, Jamaica on 10 December 1982 and which entered into force some twelve years later.8

19. Although not all states are party to the LOSC9 significant elements of the Convention are generally held to be declaratory of customary international law. The scope of the LOSC, which has been described as a ‘Constitution for the Oceans’10, is extremely broad.11

20. The LOSC balances the rights and interests of States acting in different capacities, for instance flag States, coastal States, port States, geographically disadvantaged and land-locked States as well as developed and developing States. Many of its provisions serve the interests of the international community as a whole. The latter include international communication (e.g. navigation), the sustainable use of marine living resources and the protection and preservation of the marine environment.

21. Two aspects of the LOSC are principally relevant to the issue of maritime monitoring and surveillance – (a) the maritime zones into which the oceans are divided and which affect its provisions on navigation, and in particular (b) the rules on the nationality of ships.

2.1 Maritime Zones

22. Part of the balance that the LOSC seeks to achieve is accomplished by the division of the seas and oceans into maritime zones.

23. The coastal State’s maritime zones are its internal waters, archipelagic waters (for archipelagic States only), territorial sea, contiguous zone, exclusive economic zone (EEZ) and continental shelf.12 Most coastal States have adopted legislation concerning all the maritime zones they can establish. As will be seen, the EEZ is to some extent an exception. Beyond the coastal State’s maritime zones are the high

---

7 United Nations Treaty Series vol 1833, p.3  
9 The United States of America being a case in point.  
11 Paragraph five of the preamble states that LOSC seeks to establish ‘a legal order for the seas and oceans which will facilitate international communication, and will promote the peaceful uses of the seas and oceans, the equitable and efficient utilization of their resources, the conservation of their living resources, and the study, protection and preservation of the marine environment’.  
12 In some cases, coastal States are entitled to an outer continental shelf that extends beyond the EEZ’s maximum breadth of 200 nautical miles from the baselines used for the measurement of the territorial sea.
seas (parts of which may lie above a coastal State’s (outer) continental shelf) and the deep sea-bed beyond national jurisdiction, also referred to as the ‘Area’.

24. Every coastal State has the right to establish the breadth of its territorial sea up to a limit of twelve nautical miles (nm), measured from baselines that are to be determined in accordance with the LOSC.13

![Diagram showing maritime zones]

Figure 1. The maritime zones14.

25. The LOSC recognizes a coastal State’s sovereignty within its internal waters, its territorial sea and, where applicable, archipelagic waters. A State’s authority within these maritime zones is in principle absolute, unless restricted by international law. Such authority implies the right to undertake monitoring and surveillance measures.

26. The most important restrictions included in the LOSC are the rights of all States of innocent passage for their vessels through the territorial sea (and archipelagic waters) and of transit passage through straits used for international navigation (e.g. the Strait of Dover). With limited exceptions such passage must in principle be ‘continuous and expeditious’ and it will remain ‘innocent’ as long as it is not prejudicial to the peace, good order and security of the coastal State by, for example, engaging in an activity not having a direct bearing on passage.15

13 LOSC, Article 3. There are a number of rules pertaining to straight baselines, but a ‘normal’ baseline, which must be used wherever the conditions for using straight baselines are not satisfied, is the low-water line along the coast as marked on large scale charts officially recognised by the coastal State. The LOSC does, however, allow States to draw straight baselines across the mouths of rivers, harbour entrances and bays, which, of course, have to be published in large scale charts.


15 LOSC, Article 19(2) contains a list of activities deemed prejudicial.
27. The right of innocent passage does not mean, however, a coastal State has no regulatory authority over vessels navigating through its territorial sea. The relevant provisions in the LOSC strike a balance between the interests in unimpeded navigation, uniformity in the regulation of international shipping and the protection and preservation of the marine environment in coastal areas. In particular a coastal State may adopt laws and regulations in conformity with the provisions of the LOSC and other rules of international law relating to innocent passage through the territorial sea in respect of *inter alia* the safety of navigation and the regulation of maritime traffic, the preservation of the coastal State’s environment, pollution prevention and reduction and the prevention of the infringement of its customs, fiscal, immigration or sanitary laws and regulations. Foreign ships exercising the right of innocent passage must comply with all such laws and regulations as well as to generally accept international regulations relating to the prevention of collisions at sea.\(^\text{16}\)

28. The LOSC also recognises the right of coastal States, where this is necessary for the safety of navigation, to require foreign ships exercising the right of innocent passage, to use such sea lanes and traffic separation schemes as may be designated or prescribed. In designating or prescribing such schemes, however, coastal States must among other matters take into account the recommendations of the competent international organization which, as will be seen below, is the International Maritime Organisation (IMO).\(^\text{17}\) Within those parts of the territorial sea that are straits used for international navigation (as well as archipelagic sea lanes within archipelagic waters and the surrounding territorial sea), the IMO’s positive approval for such sea lanes and traffic separation schemes is required.\(^\text{18}\)

29. Within a zone contiguous to the territorial sea whose outer limit is a maximum of 24 nm from the baselines, a coastal State has limited crime prevention and enforcement (but not legislative) powers for the purpose of customs, fiscal, immigration and sanitary matters.\(^\text{19}\)

30. Within its EEZ a coastal State has sovereign rights relating to living and non-living resources and with regard to other activities for the economic exploitation and exploration of the EEZ, such as the production of energy. A coastal State also has the necessary jurisdiction related to these sovereign rights, including rights of monitoring and surveillance relating to such activities, as well as jurisdiction for the establishment and use of artificial islands, installations and structures, marine scientific research and the protection and preservation of the marine environment.\(^\text{20}\) In so far as they concern the seabed, most of these rights also apply to the continental shelf where it extends beyond 200 nm from the baselines.

31. Within these two maritime zones, other States have the freedoms of navigation and overflight and of the laying of submarine cables and pipelines. The LOSC uses various means to balance these freedoms with the sovereign rights and jurisdiction

\(^{16}\) LOSC, Article 21.
\(^{17}\) LOSC, Article 22. The IMO is the United Nations specialised agency responsible for safety of navigation and prevention of pollution from ships.
\(^{18}\) LOSC, Articles 41(4) (straits) and 53(9) (archipelagic sealanes).
\(^{19}\) LOSC, Article 33.
\(^{20}\) LOSC Article 56(1).
of coastal States as well as with the various interests of the international community. In part this is achieved by obligations to respect each others’ rights and freedoms, by restrictions on those rights or by requiring States to agree on regulation within competent international organizations, for instance in the IMO.

32. It is important to note that the EU Member States with coasts in the Mediterranean Sea have not established EEZs there. While only a few EEZs have been established in the Mediterranean Sea (by States that are not members of the EU), in recent years several coastal States have established different types of zones for varying purposes which typically claim some subset of the rights that would be available to them through an EEZ.

33. The high seas and the Area are the international commons beyond the limits of national jurisdiction. Within the high seas, all States are entitled to exercise the freedoms that also exist in the EEZ and, in addition, the freedoms of fishing, marine scientific research and to construct artificial islands and other installations. The freedom of fishing is constrained by various obligations, including the obligation to cooperate in relation to trans-boundary and discrete high seas stocks. As regards the Area, the LOSC declares the Area and its mineral resources the common heritage of mankind, subjecting their exploitation to an international regime.

34. As regards maritime monitoring and surveillance, therefore, the situation can be summarised as follows:

(a) a coastal State has the exclusive right to undertake monitoring and surveillance within its territory including its territorial sea;
(b) a coastal State has the exclusive right to undertake monitoring and surveillance in connection with activities relating to living and non-living resources and with regard to other activities for the economic exploitation and exploration of the EEZ and the continental shelf, such as the production of energy; and
(c) all States have the implied right to undertake monitoring and surveillance in the high seas, but not to the extent of interfering with the exercise of the freedoms of the high seas by ships flying a foreign flag.

35. Finally a further type of maritime spatial division that is relevant to this report must be mentioned. These are the ‘search and rescue regions’ established pursuant to the 1979 International Convention on Maritime Search and Rescue (the SAR Convention), as amended.

36. Search and rescue regions are established in accordance with the SAR Convention solely for the purpose of coordinating marine search and rescue (SAR) activities from a rescue coordination centre. As noted in Chapter 2.1.7 of the Annex to the SAR Convention, the delimitation of such regions ‘is not related to and shall not prejudice the delimitation of any boundary between States’. In other words, the designation of SAR regions has no legal impact on maritime zones claimed pursuant to the LOSC.
2.2 The nationality and registration of ships

37. The ascription of nationality to ships is one of the most important means by which public order is maintained at sea. As well as indicating what rights a ship enjoys, and to what obligations it is subject, the nationality of a vessel indicates which State is to exercise jurisdiction over the vessel (which may be concurrent with the jurisdiction of the coastal State in a relevant maritime zone). Nationality also indicates which State is responsible in international law for the vessel in cases where an act or omission of the vessel is attributable to the State, and which State is entitled to exercise diplomatic protection on behalf of the vessel.21

38. Apart from specifying that there must be a ‘genuine link’ between the State and the vessel, the LOSC leaves it to each State to fix the conditions for the grant of its nationality to ships, for the registration of ships in its territory, and for the right to fly its flag. States usually grant their nationality to vessels by means of registration and by authorising ships to fly their flag. Thus expressions such as ‘the State of registration’ or the ‘flag State’ are for almost all purposes synonyms for the State whose nationality the vessel bears. LOSC also provides that each State must issue to ships to which it has granted the right to fly its flag documents to that effect.22

39. In practice ships can change nationality somewhat rapidly and with relative ease and the notion of the ‘genuine link’ has not been widely observed in practice. In particular a number of States, known as ‘flag of convenience’ or ‘open registry’ States, permit foreign ship owners with no real connection to them to register their ships and to fly their flag. Indeed at present a large proportion of the world’s commercial fleet is registered to flags of convenience.

40. In practice, therefore, although the LOSC requires every State to effectively exercise its jurisdiction and control in administrative, technical and social matters over ships flying its flag,23 in practice the only link that many vessels have with their flag State is the fact that they are included in the register that every flag State is required to maintain that must contain the names and particulars of ships flying its flag, except those which are excluded from generally accepted international regulations on account of their small size.

41. Partly due to the variable quality of national ship registers the IMO Ship Identification Number Scheme was introduced in 198724 and became mandatory in 1996 for all propelled sea-going merchant ships of 100 gross tonnage and over upon keel laying, excluding the following:

- vessels solely engaged in fishing;
- vessels without mechanical means of propulsion;
- pleasure yachts;
- ships engaged on special service (e.g. lightships, SAR vessels);
- hopper barges;
- hydrofoils and other air cushion vehicles;

22 LOSC, Articles 91 and 92.
23 LOSC, Article 94(1).
24 IMO Resolution A.600(15)
• floating docks and other such structures;
• ships of war and troopships; and
• wooden ships.  

42. The IMO number is made up of the letters “IMO” and a unique seven digit number assigned by Lloyds Register-Fairplay Limited (LRF) when the ship is constructed. This number must be permanently marked in a visible place on the ship’s hull or superstructure and internally.

43. Passenger ships must also ensure the identification number is marked on a horizontal surface visible from the air. The number will appear in the ship’s certificates. The sole authority for assigning IMO identification numbers is LRF which is also the sole authority for verifying numbers.

44. IMO identification numbers are never reused or reassigned. Therefore they remain unique to the ship they were first issued to. It follows that two or more vessels cannot share the same number.

45. As regards registration at the national level, in other words by the flag State, this is a matter of national law and practice. The United Kingdom (UK) shipping register is described in the following paragraphs by way of example.

46. The UK maintains a register of all ships registered as British (i.e. flying the British flag). This register is explicitly stated to be available for public inspection. The register is divided into four parts:

• Part I for all vessels which are not fishing vessels or registered on that Part restricted to small ships;
• Part II for fishing vessels;
• Part III for small ships; and
• Part IV for bareboat charter ships.

47. No ship may be registered on more than one part of the register. Any person may request a transcript of a register entry or may inspect the register itself.

48. In order to register a vessel a name must be proposed. Once this is accepted and registration is complete the ship may only be known by that name. If a vessel is being registered for the first time it will also be given an individual (national) registration number (or port number for fishing vessels).

25 SOLAS Regulation XI-1/3.
26 Ibid.
28 Ibid s.8(7).
29 Reg. 2(1), Merchant Shipping (Registration of Ships) Regulations 1993, as amended.
30 Ibid reg. 5.
31 Ibid reg. 2(3).
32 Ibid reg. 2(4).
33 Ibid reg. 30(1).
34 Ibid reg. 30(2).
35 Ibid reg. 31(2).
49. The rules relating to ships’ names dictate that no two ships on the same Part of the register may have the same or sufficiently similar names as to be likely to cause confusion. For fishing vessels, however, it may be possible to have several vessels of the same/similar name on the register providing they are registered at different ports.

50. Therefore, in the UK at least, it is possible that two or more ships might share the same name provided they are contained in different parts of the register. The registration number, is however unique and will retain with a given ship for as long as it remains registered on the UK shipping register.

---

36 ibid Sch. 1, para 2
37 ibid Sch. 1, para 3. Names may also be refused if they may cause offence or represent a clear connection to the royal family
3 Reporting regimes

51. Under this heading are included those regimes whereby data must be actively reported by a person or vessel subject to the applicable regime. As will be seen this reporting requirement may be automated or manual or both. Furthermore various different means of transmitting the relevant data are provided for depending on the regime.

52. As regards the reporting regimes that are the subject of this Study, locating the relevant legal rules and thus the data that is required to be reported is relatively straightforward. After all, in order to impose an obligation to report the reporting obligations must be specified in law at whatever level in order to impose the relevant obligations.

3.1 Vessel monitoring system for fisheries

3.1.1 Background

53. In connection with the implementation of the Common Fisheries Policy (CFP), European Community legislation provides for the establishment and operation of a satellite based ‘vessel monitoring system’ (VMS) by each Member State in order to monitor the position and movement of fishing vessels.

54. In outline this system requires each relevant fishing vessel to be fitted with a satellite tracking device. Since 1 January 2005 the fitting of such devices has been mandatory for fishing vessels exceeding 15 metres overall length.\(^{38}\)

55. Each satellite tracking device contains a geographical position measuring system, invariably the US GPS system, together with a transmitter capable of transmitting details of the position (and course) of the vessel. Such data are sent periodically via satellite to the Fisheries Monitoring Centre (FMC) that each Member State is required operate.

56. The task of the FMC of each Member State is to monitor:

(a) the fishing vessels flying the flag of that Member State regardless of the waters or port they are in;
(b) Community fishing vessels flying the flag of other Member States within the fishing waters (meaning essentially the territorial sea or EEZ) of that Member State; and
(c) third country fishing vessels during the time they are within the fishing waters of that Member State.\(^{39}\)

\(^{38}\) With the exception of fishing vessels used exclusively for the exploitation of aquaculture and operating exclusively within the baselines of Member States. Commission Regulation (EC) No. 2244/2003, Article 2.

57. VMS operates on the basis of flag State responsibility. Therefore in the case where a fishing vessel from flag Member State A is fishing in the fishing waters of coastal Member State B, the satellite signal from the vessel is transmitted via satellite to (the FMC of) Member State A and then, when the relevant coastal state is determined, relayed to the FMC of the coastal Member State B.

![Diagram of VMS components](image)

**Figure 2 – Basic components of a VMS**

### 3.1.2 Legal basis

58. The detailed rules on this topic are currently set out in Commission Regulation (EC) No 2244/2003 of 18 December 2003 laying down detailed provisions regarding satellite-based Vessel Monitoring Systems (the ‘VMS Regulation’).

59. The VMS Regulation was adopted by the European Commission pursuant to Articles 22(3) and 23 (5) of Council Regulation (EC) No 2371/2002 of 20 December 2002 on the conservation and sustainable exploitation of fisheries resources under the Common Fisheries Policy (‘the Framework Regulation’). The Framework Regulation was adopted at the time of the 2002 reform of the CFP.

60. The provisions on VMS in the Framework Regulation are somewhat brief. Article 22 (1)(b) simply states:

1. Activities within the scope of the Common Fisheries Policy shall be prohibited, unless the following requirements are met:

   - ....
(b) a fishing vessel shall have installed on board a functioning system which allows detection and identification of that vessel by remote monitoring systems. This requirement applies to vessels exceeding 18 metres length overall as from 1 January 2004 and to vessels exceeding 15 metres length overall as from 1 January 2005;

61. The original legal basis for the establishment of VMS was, however, contained in Council Regulation (EC) No 686/97 of 14 April 1997 amending Regulation (EEC) No 2847/93 establishing a control system applicable to the common fisheries policy (‘Regulation 686/97’). Regulation 686/97 introduced a new article 3 into Regulation (EEC) No 2847/93 establishing a control system applicable to the common fisheries policy (the ‘Control Regulation’).

62. Detailed provisions were then adopted by the European Commission in Commission Regulation (EC) No 1489/97 of 29 July 1997 laying down detailed rules for the application of Council Regulation (EEC) No 2847/93 as regards satellite-based vessel monitoring systems (the ‘old VMS Regulation’). The latter regulation was repealed with effect from 1 January 2004 with the entry into force of the VMS Regulation. However Article 3 of the Control Regulation remains in place.

3.1.3 What data is reported?

63. The data that must be reported by each fishing vessel that is subject to VMS is specified in Article 5 of the VMS Regulation. This states:

1. The satellite-tracking devices installed on board Community fishing vessels shall ensure the automatic transmission to the FMC of the flag Member State, at all times, of data relating to:

   (a) the fishing vessel identification;
   (b) the most recent geographical position of the fishing vessel, with a position error which shall be less than 500 metres, with a confidence interval of 99 %;
   (c) the date and time (expressed in Universal Time Coordinated (UTC)) of the fixing of the said position of the fishing vessel; and
   (d) with effect from 1 January 2006 at the latest, the speed and course of the fishing vessel.\(^\text{(40)}\)

64. More detail concerning the data that must be transmitted is contained in Annex 1 (even though Article 5 which sets out the basic reporting obligation does not specifically refer to that Annex 1). Annex 1 describes the data that must be simultaneously transmitted by the flag Member State to the FMC of a coastal Member State in whose fishing waters a vessel is located.

65. Annex 1 contains two tables that set out: (A) the content of each position report; and (B) the structure of such a report.

66. It is necessary to examine both tables in order to obtain a full picture of the data to be transmitted.

\(^\text{(40)}\) Article 5.
67. Table A provides as follows:

A. Content of position report

<table>
<thead>
<tr>
<th>Data element</th>
<th>Field code</th>
<th>Mandatory/optional</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start record</td>
<td>SR</td>
<td>M</td>
<td>System detail; indicates start of record</td>
</tr>
<tr>
<td>Address</td>
<td>AD</td>
<td>M</td>
<td>Message detail; destination; Coastal Member State Alpha-3 ISO country code</td>
</tr>
<tr>
<td>Type of message</td>
<td>TM</td>
<td>M</td>
<td>Message detail; message type, ‘POS’</td>
</tr>
<tr>
<td>Radio call sign</td>
<td>RC</td>
<td>M</td>
<td>Vessel registration detail</td>
</tr>
<tr>
<td>Trip No</td>
<td>TN</td>
<td>O</td>
<td>Activity detail; fishing trip serial number in current year</td>
</tr>
<tr>
<td>Vessel name</td>
<td>NA</td>
<td>O</td>
<td>Vessel registration detail</td>
</tr>
<tr>
<td>Internal reference No</td>
<td>IR</td>
<td>O()</td>
<td>Vessel registration detail. Unique vessel number as flag state Alpha-3 ISO country code followed by number</td>
</tr>
<tr>
<td>External registration No</td>
<td>XR</td>
<td>O</td>
<td>Vessel registration detail; the side number of the vessel</td>
</tr>
<tr>
<td>Latitude (decimal)</td>
<td>LT</td>
<td>M</td>
<td>Activity detail; position at time of transmission</td>
</tr>
<tr>
<td>Longitude (decimal)</td>
<td>LG</td>
<td>M</td>
<td>Activity detail; position at time of transmission</td>
</tr>
<tr>
<td>Speed</td>
<td>SP</td>
<td>M (²)</td>
<td>Vessel speed in tenths of knots</td>
</tr>
<tr>
<td>Course</td>
<td>CO</td>
<td>M (²)</td>
<td>Vessel course 360° scale</td>
</tr>
<tr>
<td>Date</td>
<td>DA</td>
<td>M</td>
<td>Message detail; date of transmission</td>
</tr>
<tr>
<td>Time</td>
<td>TI</td>
<td>M</td>
<td>Message detail; date of transmission</td>
</tr>
<tr>
<td>End of record</td>
<td>ER</td>
<td>M</td>
<td>System detail; indicates end of record</td>
</tr>
</tbody>
</table>
Table B, after outlining the data transmission structure provides:

<table>
<thead>
<tr>
<th>Category</th>
<th>Data element</th>
<th>Field code</th>
<th>Type</th>
<th>Contents</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>System details</td>
<td>Start record</td>
<td>SR</td>
<td></td>
<td></td>
<td>Indicates start of the record</td>
</tr>
<tr>
<td></td>
<td>End record</td>
<td>ER</td>
<td></td>
<td></td>
<td>Indicates end of the record</td>
</tr>
<tr>
<td>Message details</td>
<td>Address destination</td>
<td>AD</td>
<td>Char*3</td>
<td>ISO-3166 Address</td>
<td>Address of the party receiving</td>
</tr>
<tr>
<td></td>
<td>Type of message</td>
<td>TM</td>
<td>Char*3</td>
<td>Code</td>
<td>First three letters of the message type</td>
</tr>
<tr>
<td></td>
<td>Date</td>
<td>DA</td>
<td>Num*8</td>
<td>YYYYMMDD</td>
<td>Year, month and date</td>
</tr>
<tr>
<td></td>
<td>Time</td>
<td>TI</td>
<td>Num*4</td>
<td>HHMM</td>
<td>Hours and minutes in UTC</td>
</tr>
<tr>
<td>Vessel registration details</td>
<td>Radio call sign</td>
<td>RC</td>
<td>Char*7</td>
<td>IRCS Code</td>
<td>International radio call sign of the</td>
</tr>
<tr>
<td></td>
<td>Vessel name</td>
<td>NA</td>
<td>Char*30</td>
<td>ISO 8859,1</td>
<td>Name of the vessel</td>
</tr>
<tr>
<td></td>
<td>External registration</td>
<td>XR</td>
<td>Char*14</td>
<td>ISO 8859,1</td>
<td>Side No of the vessel</td>
</tr>
<tr>
<td></td>
<td>Internal reference No</td>
<td>IR</td>
<td>Char*3</td>
<td>Num*9</td>
<td>ISO-3166 + max.9N Unique vessel No attributed by the flag State pursuant to registration</td>
</tr>
<tr>
<td>Activity details</td>
<td>Latitude (decimal)</td>
<td>LT</td>
<td>Char*7</td>
<td>+/-DD.ddd</td>
<td>Value negative if latitude is in the southern hemisphere (1) (WGS84)</td>
</tr>
<tr>
<td></td>
<td>Longitude (decimal)</td>
<td>LG</td>
<td>Char*8</td>
<td>+/-DDDDD.d</td>
<td>Value negative if longitude is on the western hemisphere (1) (WGS84)</td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td>SP</td>
<td>Num*3</td>
<td>Knots*10</td>
<td>e.g./SP/105 = 10.5 knots</td>
</tr>
<tr>
<td></td>
<td>Course</td>
<td>CO</td>
<td>Num*3</td>
<td>360 degree scale</td>
<td>e.g./CO/270 = 270°</td>
</tr>
<tr>
<td></td>
<td>Trip No</td>
<td>TN</td>
<td>Num*3</td>
<td>001-999</td>
<td>No of the fishing trip in current year</td>
</tr>
</tbody>
</table>

69. While the Master of each fishing vessel subject to VMS is under a duty to ensure that satellite tracking devices are fully operational at all times (Article 5(1))\(^{41}\), the VMS Regulation provides that in the event that a satellite device fails to function correctly the Master of each vessel is required to transmit the position of the vessel every four hours by email, telex, fax, telephone message or radio. The format for such a transmission must be as specified in Annex 1.

70. Each Member State is required to ensure that its FMC receives this data at least once an hour from vessels flying its flag although a two hour frequency of data transmission is permitted if the technology used by that Member State permits the polling of the actual position of each vessel.

71. In other words rather than being a passive recipient of transmitted the FMC is able to send out a signal to interrogate the tracking device as to the position of the vessel.\(^{42}\) When a fishing vessel is in port it may cease transmissions providing it first notifies the FMC accordingly (and provided the next report does not show that the vessel has changed its position).

---

\(^{41}\) The Master of each relevant vessel is also required to ensure that: (a) the data are not altered in any way; (b) the antenna/e connected to the satellite tracking device are not obstructed; (c) the power supply of the device is not interrupted; and (d) that the device is not removed from the vessel (Article 5(2)).

\(^{42}\) The Member States have a choice as to the technology used for their VMS and as regards the satellite tracking devices used. Not all of the technology permits polling.
72. Additional rules require the FMC to be notified of the date and time of entry into certain specified areas including waters where specific rules on access and resources apply, the regulatory areas of certain regional fisheries organisations on the high seas and the waters of third countries.

73. Similar rights and obligations are created with regard to third country fishing vessels within Community Waters.

3.1.4 Analysis of the data reported

74. In considering the data transmitted the categories that are of most relevance to the issues considered in this Study are those placed under the heading ‘vessel registration details’ in the definition of the data elements. These are: (a) ‘radio call sign’ which is defined as the ‘international radio call sign of the vessel’; (b) ‘vessel name’, which is defined as ‘name of the vessel’; (c) ‘external registration’, defined as the ‘side number of the vessel’; and (d) ‘internal reference no’ which is defined as the ‘unique vessel no. attributed by the flag state pursuant to registration’.

3.1.4.1 Registration details

75. In order to understand the content and implications of these data it is necessary to examine several other instruments of the CFP.

76. The most logical starting point is Article 15 of the Framework Regulation which in outline requires each Member State to keep a register of fishing vessels flying its flag and the Commission to set up a Community fishing fleet register on the basis of the national registers.

77. Article 15(1) specifies that each national register must include ‘the minimum information on vessel characteristics that is necessary for the management of measures established at Community level’. Article 15(3) also requires the Commission to make the Community fishing vessel register available to Member States, while at the same time complying with ‘Community provisions regarding the protection of personal data’.

78. The provisions of Article 15 were further developed in Commission Regulation (EC) No. 26/2004 of 30 December 2003 on the Community fishing fleet register (‘the Register Regulation’).

79. Article 1(1) of the Register Regulation states:

1. This Regulation:
   (a) determines the minimum information on vessel characteristics and activity which must figure in the register which each Member State keeps of the fishing vessels flying its flag (hereinafter called ‘the national register’);
   (b) lays down the obligations of Member States regarding the collection, validation and transmission of the data from their national register to the Commission;
   (c) lays down the obligations of the Commission regarding the management of the Community fishing fleet register (hereinafter called ‘the Community register’).
80. Three points in particular need to be made about this regulation.

81. First of all, notwithstanding Article 1(1)(a) and the fact that paragraph 3 of the recitals records the need to identify the information to be included in the national registers, the regulation does not actively identify the minimum contents of national registers. That this is as specified in Annex 1 is rather to be inferred.

82. Second, the regulation provides in Article 10 for each fishing vessel (and the regulation applies to all Community fishing vessels including those used for aquaculture) to have a unique community fleet register (CFR) number that must be assigned definitively when each vessel is first registered in a national register and which must be ‘included in all transmissions of data between the Member States and the Commission concerning the characteristics and activities of fishing vessels’. As defined in Annex each CFR number must comprise the first three letters of the name of the Member State (Alpha—3 ISO Code) followed by an identifying series (nine characters). If the series has fewer than nine characters ‘additional zeros must be inserted on the left hand side’.

83. Third, the contents of the Community register are different to those of the national registers. In particular details of vessel owners and agents are omitted from the Community register.

84. The contents of the national registers, as specified in Annex 1 are as follows:

<table>
<thead>
<tr>
<th>Name of zone</th>
<th>Maximum number of characters</th>
<th>Alignment L(eft)/R(ight)</th>
<th>Definition and comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of registration</td>
<td>3</td>
<td>—</td>
<td>Member State (Alpha—3 ISO code) in which vessel is registered for fishing pursuant to Regulation (EC) No 2371/2002. Always the reporting country.</td>
</tr>
<tr>
<td>CFR (2)</td>
<td>12</td>
<td>—</td>
<td>Unique identification number of a fishing vessel. Member State (Alpha—3 ISO code) followed by an identifying series (nine characters). Where a series has fewer than nine characters, additional zeros must be inserted on the left hand side.</td>
</tr>
<tr>
<td>Event code</td>
<td>3</td>
<td>—</td>
<td>Code identifying the type of event reported. (Table 1)</td>
</tr>
<tr>
<td>Date of event(3)</td>
<td>8</td>
<td>—</td>
<td>Date (YYYYMMDD) on which event occurred</td>
</tr>
<tr>
<td>Licence indicator</td>
<td>1</td>
<td>—</td>
<td>Vessel with a fishing licence according to Regulation (EC) No 3690/93: V(Yes)/N(No)</td>
</tr>
<tr>
<td>Registration number</td>
<td>14</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td>External marking</td>
<td>14</td>
<td>L</td>
<td>Pursuant to Regulation (EEC) No 1381/87</td>
</tr>
<tr>
<td>Name of vessel</td>
<td>40</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Length</td>
<td>Recommended Unit</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port of registration</td>
<td>5</td>
<td>L</td>
<td>National code</td>
</tr>
<tr>
<td>IRCS indicator</td>
<td>1</td>
<td>—</td>
<td>Vessel with an international radio on board: Y (Yes)/N (No)/U (Unknown)</td>
</tr>
<tr>
<td>IRCS</td>
<td>7</td>
<td>L</td>
<td>(International radio call sign). International radio call sign</td>
</tr>
<tr>
<td>VMS indicator</td>
<td>1</td>
<td>—</td>
<td>Vessel with a satellite monitoring system in accordance with Article 22 of Regulation (EC) No 2371/2002: Y (yes)/N (No)</td>
</tr>
<tr>
<td>Main fishing gear (5)</td>
<td>3</td>
<td>L</td>
<td>Code of main gear (Table 3)</td>
</tr>
<tr>
<td>Subsidiary fishing gear</td>
<td>3</td>
<td>L</td>
<td>Code of subsidiary gear (Table 3)</td>
</tr>
<tr>
<td>LOA</td>
<td>6</td>
<td>R</td>
<td>(Length over all) Length over all in metres, defined in accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>LBP</td>
<td>6</td>
<td>R</td>
<td>(Length between perpendiculars) Length between perpendiculars in metres, defined in accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>Tonnage GT</td>
<td>8</td>
<td>R</td>
<td>In GT, defined in accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>Other tonnage(6)</td>
<td>8</td>
<td>R</td>
<td>In tonnes according to the Oslo Convention or in accordance with a definition to be laid down by the Member State.</td>
</tr>
<tr>
<td>GTs (6)</td>
<td>7</td>
<td>R</td>
<td>In GT, an increase in tonnage permitted on grounds of safety pursuant to Article 11 of Regulation (EC) No 2371/2002.</td>
</tr>
<tr>
<td>Power of main engine(6)</td>
<td>8</td>
<td>R</td>
<td>In kW, in accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>Power of auxiliary engine (6)</td>
<td>8</td>
<td>R</td>
<td>In kW. Includes all installed engine power not included under the heading ‘Power of main engine.’</td>
</tr>
<tr>
<td>Hull material</td>
<td>1</td>
<td>—</td>
<td>Code (Table 4)</td>
</tr>
<tr>
<td>Year of commissioning</td>
<td>4</td>
<td>—</td>
<td>In accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>Month of commissioning</td>
<td>2</td>
<td>—</td>
<td>In accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>Day of commissioning</td>
<td>2</td>
<td>—</td>
<td>In accordance with Regulation (EEC) No 2930/86.</td>
</tr>
<tr>
<td>Segment</td>
<td>3</td>
<td>—</td>
<td>Code (Table 5)</td>
</tr>
<tr>
<td>Country of importation/ exportation</td>
<td>3</td>
<td>—</td>
<td>Alpha—3 ISO code for the importing or exporting country.</td>
</tr>
<tr>
<td>Type of export</td>
<td>2</td>
<td>—</td>
<td>Code (Table 6)</td>
</tr>
<tr>
<td>Code for public aid</td>
<td>2</td>
<td>—</td>
<td>Code (Table 7)</td>
</tr>
<tr>
<td>Date of administrative decision</td>
<td>8</td>
<td>—</td>
<td>Date (YYYYMMDD) of the administrative decision referred to in Regulation (EC) No 1438/2003, Article 6.</td>
</tr>
<tr>
<td>Segment covered by administrative decision</td>
<td>3</td>
<td>—</td>
<td>Code of MAGP segment to be notified in accordance with Regulation (EC) No 1438/2003.</td>
</tr>
<tr>
<td>Year of construction</td>
<td>4</td>
<td>—</td>
<td></td>
</tr>
</tbody>
</table>
85. Annex II contains the ‘events’ that must be notified periodically by the Member States to the Commission so that the Community register can be updated is as follows:

**ANNEX II**

**DATA TO BE PROVIDED DEPENDING ON THE TYPE OF EVENT DEFINED IN ANNEX I, TABLE I**

<table>
<thead>
<tr>
<th></th>
<th>Entry to fleet</th>
<th>Within fleet</th>
<th>Exit from fleet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CEN</td>
<td>CST</td>
<td>CHA</td>
</tr>
<tr>
<td>Country of registration</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CFR</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Event code</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Date of event</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Licence indicator (1)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Registration number</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>External marking</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Name of vessel</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Port of registration</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IRCS indicator</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IRCS (2)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>VMS indicator (1)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Main fishing gear</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Subsidiary fishing gear</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>LOA ((1))((3))</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>----------------</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td>LBP ((3))</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Gross tonnage GT ((1))((5))</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Other tonnage ((4))</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>GTs</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Power of main engine</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Power of auxiliary engine</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hull material</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Year of commissioning((6))</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Month of commissioning</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Day of commissioning</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Segment</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Country of importation/exportation</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Type of export ((1))</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Code for public aid</td>
<td>—</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Date of administrative decision ((12))</td>
<td>—</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry to fleet</th>
<th>Within fleet</th>
<th>Exit from fleet</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEN</td>
<td>CST</td>
<td>CHA</td>
</tr>
</tbody>
</table>

| Segment covered by administrative decision | X | X | X | — | — | — | — |

86. In other words the data that is more evidently of a personal nature is not reported to the Commission although the unique CFR number is.

87. It is interesting to note that the Register Regulation specifically refers to data protection issues. These are contained in Article 11 which is titled ‘Access’. This article, in its entirety, states:

1. The Member States shall have access to all the information contained in the Community register on condition that they comply with the provisions relating to the protection of personal data arising from Regulation (EC) No 45/2001, and in particular Article 8 thereof.

2. The public shall have access to a version of the Community register which does not contain personal data.

3. Requests for access to personal data in the Community register shall be dealt with by the Commission in accordance with the provisions of Regulation (EC) No 45/2001.

88. Before turning to the actual content of the Community register it is also necessary to consider the rules pertaining to the external marking of Community fishing vessels.
89. These are contained in a rather old regulation, albeit one that apparently remains in force, namely Commission Regulation (EEC) No 1381/87 of 20 May 1987 establishing detailed rules concerning the marking and documentation of fishing vessels.

90. Article 1 of this regulation states:

Fishing vessels flying the flag of, or registered in, a Member State shall be marked as follows:

1. The letter(s) of the port or district in which the vessel is registered and the number(s) under which it is registered shall be painted or displayed on both sides of the bow, as high above the water as possible so as to be clearly visible from the sea and the air, in a colour contrasting with the ground on which they are painted.

For vessels over 10 metres but not over 17 metres in length, the height of the letters and numbers shall be at least 25 centimetres with a line thickness of at least 4 centimetres. For vessels over 17 metres in length, the height of the letters and numbers shall be at least 45 centimetres, with a line thickness of at least 6 centimetres.

The flag State may require the international radio call sign (IRCS), or the letters and numbers of registration, to be painted on top of the wheelhouse, so as to be clearly visible from the air, in a colour contrasting with the ground on which it is painted.

91. Subsequent articles go on to describe aspects of vessel marking and documentation that are not relevant to this discussion.

92. It follows that each community fishing vessel has three unique identification numbers. These are: (a) the CFR number; (b) the national registration number; and (c) the external registration or side number of the vessel. All three of these numbers are included in the Community Register.

93. Thus to take a random example from the Community Register, the CFR of the French vessel Rohellan is FRA000115934 while her national registration number is 115934. Because this vessel is registered at Lorient her external registration number is LO 11594.

94. In other words in France the national registration number forms part of both the CFR and the side number.

95. The Member States are, however, free to determine the basis on which national registration numbers are allocated. Thus to take another random example the German trawler Moeve, which is registered at the port of Freest, has: (a) the CFR number DEU000020614; (b) the national registration number FRE 3; and (c) the side number FRE 3.

96. Returning to the VMS Regulation, therefore, the reference to the ‘internal reference number’ should be understood to be the CFR number which under the regulation that preceded the Regulation Registration (Commission Regulation (EC) No 2090/98) was known as the ‘Internal Number’.

3.1.4.2 Radio call sign

97. The assignment of international call signs (i.e. those for countries), along with things like frequencies, is the prerogative of the Radio Regulations (current version is 2004). The Radio Regulations are administered by the International Telecommunications Union (ITU) which is a specialised agency of the United Nations within which the public and private sectors co-ordinate global
telecommunication issues and services. The Radio Regulations, which are amended or updated through the World Radio-communication Conferences, are effectively an intergovernmental treaty. The individual international call signs can be found in Appendix 42.43

98. As regards national practice the example of the UK is once again provided. Call signs are allocated to vessels when they are first issued with a Ship Radio Licence (which must be applied for via the telecommunications regulator OFCOM). This uniquely identifies the vessel within the International Maritime Mobile Service. All merchant vessels with a “built in” radio registered in the UK must have a Ship Radio Licence.

99. Vessels that use only portable VHF radios (i.e. those with an integral antenna) require a Ship Portable Radio Licence, for which a T-number (a UK specific call sign) rather than a call sign is allocated. Such radios can then be used on several vessels.

100. An allocated vessel call sign remains with the vessel for the duration of its life, regardless of changes in either ownership or name (the call sign will be surrendered if the vessel is no longer registered in the UK or is unlicensed for 2 years or more). Call signs cannot be transferred between vessels.

3.1.5 Why is the data reported?

101. Article 13 (1) of the VMS Regulation states that data received is to be used for the ‘effective monitoring of the fishing activities of vessels’.

102. This Article goes on to require flag Member States to ensure that the data they receive from fishing vessels flying their flags are recorded in computer readable form for a period of three years. A similar obligation is imposed on Coastal Member States in respect of data received from flag Member States.

3.1.6 Who has a right to the data?

3.1.6.1 The flag Member State

103. As already described, pursuant to the VMS Regulation each flag Member State has the right, through its FMC, to data received from all vessels flying its flag wherever they are located.

3.1.6.2 The coastal Member State in respect of Community fishing vessels in its fishing waters

104. In addition the FMC of a coastal Member State is entitled to receive from data in respect of fishing vessels within its waters that are flying the flag of other Member States from the relevant FMC.

43 http://life.itu.int/radioclub/rr/rrcont.htm
3.1.6.3 The European Commission

105. Article 14(1) of the VMS Regulation also requires the Member States to ensure that the Commission has, on specific request, remote access ‘by online sessions to the computer files containing the data recorded by’ their respective FMCs.

106. In addition it is currently planned that VMS data will be forwarded to the Community Fisheries Control Agency although no specific legal provision has so far been made in this respect.

3.1.7 Data sharing in practice

107. As the VMS regime is purely a creature of Community law it follows that international law places no restrictions on the sharing of VMS data.

108. As regards Community law, Article 14 (2) of the VMS Regulation states that the ‘data received in the framework of this Regulation shall be treated in a confidential manner’. The precise meaning of the notion of treating data in a confidential manner is open to interpretation.

109. The Framework Regulation is silent on the issue of the confidentiality of VMS data as is Article 3 of the Control Regulation. Equally the earlier (now repealed) implementing regulation says nothing about confidentiality.

110. In practice the issue of confidentiality lies at the heart of much of the debate regarding the use and treatment of VMS data. For the operators and owners of fishing vessels knowing in real time precisely where competitors are fishing is potentially valuable information. Consequently on the part of the industry there is a keen desire to keep this information as secret as possible. Software exists for ‘spoofing’ the position data and unsealed tracking devices can be vulnerable to tampering. Another practice in some fisheries is to place a metal bucket over the device shortly before fishing is due to start so as to delay the transmission of data.

111. The manner in which the FMCs are operated reflects cultural attitudes towards secrecy and arguably the relative power of the fishing lobby in each country. In some Member States security in and around FMCs is extremely strict with locked door and strict access policies to what are effectively sealed operations rooms. A leaflet published by the ministry responsible for Spain’s FMC states:

The FMC has been constructed following strict rules on data confidentiality and protection. Access to the center and the terminals is restricted to authorised personnel. Data access is also protected by random identifying system and a password. Each user can only accede to the data and functions needed for his work.

We are nowadays setting forth the FMC Safety Certificate according to ISO/IEC DIS 14980 regulations.

112. Elsewhere the FMC comprises little more than a few computer terminals (albeit password protected) in the corner of a regular office.

113. From a surveillance perspective VMS data has the potential to contribute towards building the overall maritime picture although the delays between regular transmission mean that something less than ‘real-time’ positioning is provided.
114. At present it is up to the Member States to determine how or whether to share VMS data among different agencies or cross borders beyond the minimum requirements set out in the regulation.

115. In Spain, for example, the two ministerial orders adopted to give effect to VMS requirements imposed by the VMS Regulation and the old VMS Regulation respectively include clear provisions on confidentiality. Order No. 26923 of 12 November 1998 of the Ministry of Agriculture, Fisheries and Food *por la que se regula en España el sistema de localización de buques pesqueros vía satélite* (the Spanish rules and regulations for fishing vessel satellite location systems) states:

First additional provision. Confidentiality.

All information about the movements and activities of vessels acquired through the satellite tracking system (VMS) covered by this provision will remain strictly confidential, and its sole purpose is the control of fishing activity by the competent authorities.\(^{44}\)

116. At the national level VMS data are usually only made available in practice for fisheries enforcement authorities. However customs, law enforcement, and the military are also interested in VMS data. Nevertheless wide variations exist.

117. Unsurprisingly in Spain access to VMS data by other agencies is strictly controlled and such data is only provided in the context of ongoing criminal investigations. A similarly restrictive approach is found in Germany.

118. On the other hand VMS data is routinely fed into Finland’s maritime surveillance data sharing mechanism (which is described in more detail below) and in the UK VMS data is made available to other agencies for the purposes of management, monitoring and control of the CFP and for other management, control and enforcement functions (see Section 6.2.7 below).

3.2 **AIS (automatic identification system)**

3.2.1 Background

119. An ‘Automatic Identification System’ (AIS) is a ship born mechanism that automatically provides for the exchange of information between ships as well as the provision of such data to coastal stations.

120. Each AIS consists of transponder unit that includes a GPS geographical position measuring system, a VHF transmitter/receiver and a display/terminal. The unit broadcasts a message at regular intervals that sets out the identification,
position, speed, and course of the ship in addition to certain detailed items about the ship and its cargo.

121. This message can then be picked up by other ships (as well as coastal stations) within VHF range (which is essentially line of sight) which in turn send their own messages. Through an automatic protocol, called SOTDMA, no two transmitters within range of each other transmit at the same time.\textsuperscript{45}

122. The frequency of AIS transmissions increases with speed as set out in the following table\textsuperscript{46}.

<table>
<thead>
<tr>
<th>Type of ship</th>
<th>General reporting interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship at anchor</td>
<td>3 min</td>
</tr>
<tr>
<td>Ship 0-14 knots</td>
<td>12 sec</td>
</tr>
<tr>
<td>Ship 0-14 knots and changing course</td>
<td>4 sec</td>
</tr>
<tr>
<td>Ship 14-23 knots</td>
<td>6 sec</td>
</tr>
<tr>
<td>Ship 14-23 knots and changing course</td>
<td>2 sec</td>
</tr>
<tr>
<td>Ship &gt;23 knots</td>
<td>3 sec</td>
</tr>
<tr>
<td>Ship &gt;23 knots and changing course</td>
<td>2 sec</td>
</tr>
</tbody>
</table>

123. The initial purpose of AIS was to enable ship to ship transmissions in order to prevent collisions. The fact that it enables a ship to learn the identity of other ships within the vicinity is an improvement over radar which simply sends back an echo signal.

124. AIS has been promoted by the International Maritime Organization (IMO). In accordance with the latest International Convention for the Safety of Life at Sea (SOLAS)\textsuperscript{47} of 1974, which was negotiated under the auspices of the IMO and, as will be seen below, it is currently mandatory for ships over 300 gross tonnage.\textsuperscript{48}

125. Two separate sets of technical standards have in fact been developed for AIS: AIS A and AIS B. The focus of the discussion that follows is on the mandatory IMO AIS which uses AIS A.

126. AIS B is a non-mandatory standard that is marketed for use by smaller vessels, primarily pleasure craft, that are not subject to mandatory AIS.\textsuperscript{49} In part due to its cost, but also because it is not mandatory, uptake of AIS B has been relatively

\textsuperscript{45} European Commission/Joint Research Centre Survey of Maritime Surveillance Systems Ispra, Italy, 6 December 1997. SOTDMA stands for self organising time division multiple access. Some AIS B units also use SOTDMA. Others use a separate protocol called CSTDMA.

\textsuperscript{46} To be precise the frequency of navigation data transmissions increases with speed: the static data is transmitted at six minute intervals.

\textsuperscript{47} The 1974 SOLAS is the latest in a series of SOLAS conventions, the first of which was inspired by the sinking of the Titanic

\textsuperscript{48} In the United States it is currently proposed to make AIS compulsory for all vessels of 65 feet length overall.

\textsuperscript{49} In broad terms AIS equipment that complies with the B technical standards is simpler, uses less power and operates over a shorter range. The technical standards for AIS A and AIS B are developed by the ITU and the IEC.
limited to date. However signals from AIS B are picked up by other vessels as well as coastal stations.

Figure 3 – AIS System

127. In part due to the paucity of enforcement mechanisms available to the IMO this is an area in respect of which the European Community has legislated even though it is not a member of the IMO. Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (‘the VTM Directive’) contains a number of provisions relating to AIS.

128. Specifically pursuant to Article 9 of the VTM Directive each Member State was required to set up appropriate equipment and shore based installations for receiving and using AIS information by the end of 2007. It is understood that most Member States were able to comply with this deadline.

3.2.2 Legal basis

3.2.2.1 SOLAS

129. The basic obligation to fit and use AIS is imposed by Regulation 19 of Chapter V of SOLAS which is entitled ‘Safety of Navigation’. All of the coastal Member States are party to SOLAS.

130. The AIS provisions were originally developed at the 73rd session of IMO’s Maritime Safety Committee (MSC) between 27 November and 6 December 2000. They were originally to come into force on 1 July 2002 but were then put back to 1 July 2004 (excluding passenger ships and tankers, which were required to comply by 1 July 2003).

---

50 According to AIS Live Limited its network typically receives only a few hundred AIS B signals a day in comparison to some 25,000 signals from vessels with AIS A.
131. Pursuant to article 2.4 of Regulation 19 all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size are required to be fitted with an AIS.\textsuperscript{51} This obligation was introduced in a phased manner with various deadlines being applied to different classes of ship. With the exception of ships that were constructed before 1 July 2002 and which are not engaged in international voyages these deadlines have at the time of writing all been passed.\textsuperscript{52}

132. Warships and other government-owned vessels on non-commercial service are exempted from the requirements of Chapter V of SOLAS although Governments are encouraged to act in a manner consistent, so far as reasonable and practicable, with its provisions. In practice warships are typically fitted with AIS even if they may switch it off from time to time as necessary for operational reasons.

133. Pursuant to article 2.4.5 AIS must:
   .1 provide automatically to appropriately equipped shore stations, other ships and aircraft information, including the ship's identity, type, position, course, speed, navigational status and other safety-related information;
   .2 receive automatically such information from similarly fitted ships;
   .3 monitor and track ships; and
   .4 exchange data with shore-based facilities;

134. SOLAS goes on to provide that AIS shall be operated taking into account the guidelines adopted by the IMO. These are the \textit{Guidelines for the onboard operational use of ship-borne Automatic Identification Systems (AIS)} adopted by the IMO by Resolution A.917(22) (the ‘AIS Guidelines’).

\textbf{3.2.2.2 The VTM Directive}

135. The topic of AIS is first addressed in Article 6 of the VTM Directive. This states

\begin{enumerate}
\item Any ship calling at a port of a Member State must, in accordance with the timetable set out in Annex II(I), be fitted with an AIS which meets the performance standards drawn up by the IMO.
\item Ships fitted with an AIS, shall maintain it in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.
\end{enumerate}

136. It is to be noted that: (a) the scope of the VTM Directive is broader than that of SOLAS given that it also applies to vessels calling at Member State ports; and (b) the VTM Directive refers back to the provisions contained in SOLAS. A complex phase-in procedure is also set out, the dates of which have now been passed.

---

\textsuperscript{51} Regulation 1.4 of Chapter V of SOLAS provides that it is for each flag state government to determine to what extent the provisions of Regulation 19, are not to apply to the following categories of ships: .1 ships below 150 gross tonnage engaged on any voyage; .2 ships below 500 gross tonnage not engaged on international voyages; and .3 fishing vessels.

\textsuperscript{52} Ships that were constructed before 1 July 2002 and which are not engaged in international voyages must install an AIS by 1 July 2008.
137. Furthermore the VTM Directive requires all passenger ships to be equipped with AIS irrespective of size unless they: (a) are engaged in domestic trade; and (b) are specifically exempted by the flag Member State.

138. The only other references to AIS in the VTM Directive are contained in Article 9 which is entitled ‘Infrastructure for ship reporting systems, ships’ routing’ and which requires each coastal Member State to establish shore based AIS monitoring stations. It states:

1. Member States shall take all necessary and appropriate measures to provide themselves gradually, on a time-schedule compatible with the timetable set out in Annex II(1), with appropriate equipment and shore-based installations for receiving and utilising the AIS information taking into account a necessary range for transmission of the reports.

2. The process of building up all necessary equipment and shore-based installations for implementing this Directive shall be completed by the end of 2007. Member States shall ensure that the appropriate equipment for relaying the information to, and exchanging it between, the national systems of Member States shall be operational at the latest one year thereafter.

3.2.2.3 ITU

139. At the ITU World Radio-communication Conference (WRC) in Geneva during October/November 1997, IMO requested that two maritime VHF channels be assigned for AIS. These were designated and a footnote was added to Appendix S18 of the ITU Radio Regulations entitled “Table of Transmitting Frequencies in the VHF Maritime Mobile Band” as follows:

These channels (AIS 1 and AIS 2) will be used for an automatic ship identification and surveillance system capable of providing worldwide operation on high seas, unless other frequencies are designated on a regional basis for this purpose.

140. The channels allocated are: AIS 1 (161.975 MHz) and AIS 2 (162.025 MHz).

3.2.3 What data is reported?

141. The AIS Guidelines specify that:

The AIS information transmitted by a ship is of three different types:

- fixed or static information, which is entered into the AIS on installation and need only be changed if the ship changes its name or undergoes a major conversion from one ship type to another;
- dynamic information, which, apart from ‘Navigational status’ information, is automatically updated from the ship sensors connected to AIS; and
- voyage-related information, which might need to be manually entered and updated during the voyage.

142. Details of these information types are set out as follows. The static information is mostly set on the installation of the AIS.
### Information item Information generation, type and quality of information

<table>
<thead>
<tr>
<th>Static</th>
<th></th>
</tr>
</thead>
</table>
| MMSI (Maritime Mobile Service Identity) | Set on installation  
Note that this might need amending if the ship changes ownership |
| Call sign and name | Set on installation  
Note that this might need amending if the ship changes ownership |
| IMO Number | Set on installation |
| Length and beam | Set on installation or if changed |
| Type of ship | Select from pre-installed list |
| Location of position-fixing antenna | Set on installation or may be changed for bi-directional vessels or those fitted with multiple antennae |

143. Maritime Mobile Service Identity (MMSI) numbers are only issued when DSC (Digital Selective Calling) and or Ship Earth Station (SES) equipment is fitted on a vessel. This will happen when either an application for a new Ship Radio Licence or an amendment to the equipment on board a vessel with an existing licence is made. The process of allocating MMSI numbers is overseen by the ITU.

144. Detailed guidance for the assignment and conservation of MMSI numbers is contained in Recommendation M.585-4 *Assignment and use of maritime mobile service identities* which was last updated in 2007 (the MMSI recommendation). The most recent version of the MMSI recommendation was adopted by the ITU Radiocommunication Assembly in 2007.

145. There are four kinds of MMSI number: (a) Ship station identities; (b) Group ship station identities; (c) Coast station identities; and (d) Group coast station identities.

146. Each MMSI number is a unique series of nine digits which can be transmitted over the radio path in order to identify ship stations, ship earth stations, coast stations, coast earth stations, and group calls. These identities are formed in such a way that the identity or part thereof can be used by telephone and telex subscribers connected to the general telecommunications network principally to call ships automatically.

147. MMSI numbers allocated to ships that are equipped with *inter alia* AIS are also composed of a nine digit unique ship station identity in the format M1I2D3X4X5X6X7X8X9, where in the first three digits represent the Maritime Identification Digits (MID) and X is any figure from 0 to 9. The MID denotes the geographical area of the administration responsible for the ship station. Essentially a single MID is allocated to each country (although there is provision for the allocation of additional MIDs if needed).
148. Most of the dynamic information is entered automatically.

<table>
<thead>
<tr>
<th>Dynamic</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship’s position with accuracy indication and integrity status</td>
<td>Automatically updated from the position sensor connected to AIS The accuracy indication is for better or worse than 10 m.</td>
</tr>
<tr>
<td>Position Time stamp in UTC</td>
<td>Automatically updated from ship’s main position sensor connected to AIS</td>
</tr>
<tr>
<td>Course over ground (COG)</td>
<td>Automatically updated from ship’s main position sensor connected to AIS, if that sensor calculates COG This information might not be available</td>
</tr>
<tr>
<td>Speed over ground (SOG)</td>
<td>Automatically updated from the position sensor connected to AIS This information might not be available</td>
</tr>
<tr>
<td>Heading</td>
<td>Automatically updated from the ship’s heading sensor connected to AIS</td>
</tr>
<tr>
<td>Navigational status</td>
<td>Navigational status information has to be manually entered by the OOW and changed as necessary, for example:</td>
</tr>
<tr>
<td></td>
<td>- underway by engines</td>
</tr>
<tr>
<td></td>
<td>- at anchor</td>
</tr>
<tr>
<td></td>
<td>- not under command (NUC)</td>
</tr>
<tr>
<td></td>
<td>- restricted in ability to manoeuvre (RIATM)</td>
</tr>
<tr>
<td></td>
<td>- moored</td>
</tr>
<tr>
<td></td>
<td>- constrained by draught</td>
</tr>
<tr>
<td></td>
<td>- aground</td>
</tr>
<tr>
<td></td>
<td>- engaged in fishing</td>
</tr>
<tr>
<td></td>
<td>- underway by sail</td>
</tr>
<tr>
<td></td>
<td>In practice, since all these relate to the COLREGs, any change that is needed could be undertaken at the same time that the lights or shapes were changed</td>
</tr>
<tr>
<td>Rate of turn (ROT)</td>
<td>Automatically updated from the ship’s ROT sensor or derived from the gyro This information might not be available</td>
</tr>
</tbody>
</table>

149. The third element, voyage related information, is entered manually. As a result it is the least reliable AIS data element. Indeed even if the destination and estimated time of arrival (ETA) are correctly entered cargo information is often left blank.

<table>
<thead>
<tr>
<th>Voyage-related</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ship’s draught</td>
<td>To be manually entered at the start of the voyage using the maximum draft for the voyage and amended as required (e.g. – result of de-ballasting prior to port entry)</td>
</tr>
<tr>
<td>Hazardous cargo (type)</td>
<td>To be manually entered at the start of the voyage confirming whether or not hazardous cargo is being carried, namely:</td>
</tr>
<tr>
<td></td>
<td>- DG (Dangerous goods)</td>
</tr>
<tr>
<td></td>
<td>- HS (Harmful substances)</td>
</tr>
<tr>
<td></td>
<td>- MP (Marine pollutants)</td>
</tr>
<tr>
<td></td>
<td>Indications of quantities are not required</td>
</tr>
<tr>
<td>Destination and ETA</td>
<td>To be manually entered at the start of the voyage and kept up to date as necessary</td>
</tr>
<tr>
<td>Route plan (waypoints)</td>
<td>To be manually entered at the start of the voyage, at the discretion of the master, and updated when required</td>
</tr>
</tbody>
</table>
150. Finally provision is made within AIS for the inclusion of short safety-related messages.

| Short safety-related messages | Free format short text messages would be manually entered, addressed either a specific addressee or broadcast to all ships and shore stations |

3.2.4 Why is the data reported?

151. Neither the VTM Directive nor SOLAS contain an explicit statement as to why AIS data is gathered. It seems reasonable to infer, given the overall objective of SOLAS, that safety of navigation is an important objective. Paragraph 7 of the Recitals to the VTM Directive notes the technological progress in the area of AIS systems ‘for enhanced ship monitoring’ and the importance of inter alia AIS equipment in preventing shipping accidents.

152. However, IMO Resolution MSC. 74 (69) (May 12, 1998) states that AIS should “improve the safety of navigation by assisting in the efficient navigation of ships, protection of the environment, and operation of Vessel Traffic Services (VTS), by satisfying the following functional requirements: (a) in a ship-to-ship mode for collision avoidance, and (b) as a means for littoral States to obtain information about a ship and its cargo; and as a VTS tool, i.e. ship-to-shore (traffic management)”. 

3.2.5 Who has a right to the data?

3.2.5.1 Other vessels

153. Implicit in the structure of AIS is that other vessels within transmission range have the right to AIS information. Indeed this is the entire purpose of AIS and the reason why the radio signals sent out by an AIS are not encrypted.

3.2.5.2 Coastal States

154. Equally, implicit in the structure for the implementation of AIS foreseen by the VTM Directive is that coastal states also have a right to receive the transmitted data via their own coastal stations, required pursuant to Article 9. Furthermore it will be recalled that Article 9(2) states:

The process of building up all necessary equipment and shore-based installations for implementing this Directive shall be completed by the end of 2007. Member States shall ensure that the appropriate equipment

53 The term ‘coastal station’ is defined in Article 3 (n) in terms of a number of maritime activities that are addressed in the VTM Directive. Specifically the definition states: “coastal station’ means any one following, designated by Member States pursuant to this Directive: a vessel traffic service; a shore-based installation responsible for a mandatory reporting system approved by the IMO; or a body responsible for coordinating search and rescue or operations to tackle pollution at sea”.

31
for relaying the information to, and exchanging it between, the national systems of Member States shall be operational at the latest one year thereafter.

155. In other words the VTM Directive expressly provides for the exchange of *inter alia* VMS data between the Member States. However, Article 24 of the VTM Directive states:

> Member States shall, in accordance with their national legislation, take the necessary measures to ensure the confidentiality of information sent to them pursuant to this Directive.

### 3.2.5.3 Private persons

156. Because AIS transmissions take place on the basis of open frequencies a number of private companies have set up their own coastal monitoring stations to provide AIS information on a commercial basis over the internet usually on a subscription basis. The example of AISLive Limited is described in Section 5.4 below.

157. Nevertheless the information contained in AIS transmissions is considered to be potentially sensitive. In December 2004 the IMO’s Maritime Safety Committee (MSC) ‘condemned the regrettable publication on the world wide web or elsewhere’ of hobbyist decoded AIS data and ‘condemned those who irresponsibly publish AIS data transmitted by ships on the world-wide web, or elsewhere, particularly if they offer services to the shipping and port industries.’[^54]

### 3.2.6 Data sharing in practice

158. In practice, as will be seen below, AIS is relatively widely shared through a range of data sharing mechanisms including the French and Finnish national data sharing mechanisms, the VRMTC and NATO’s MSSIS as well as regional AIS data sharing mechanisms such as the HELCOM AIS Network. In the UK for example, the Marine and Coastguard Agency routinely forwards AIS data to state agencies including the Royal Navy, government departments including the Department for the Environment Fisheries and Rural Affairs (DEFRA) and the Police.

159. Finally the Finnish Maritime Administration has recently taken a decision to supply raw AIS data to a commercial AIS operator. The view was taken that the data does not fall into any of the exceptions provided for in the 1999 Freedom of Information Act and that there was therefore no lawful reason not to supply it.

### 3.3 LRIT

#### 3.3.1 Background

160. Long-Range Identification and Tracking of Ships (LRIT) is a new long-range vessel monitoring system that was adopted through IMO Resolution MSC 202 (81)

[^54]: 79th session of the MSC. http://www.imo.org/Safety/mainframe.asp?topic_id=110&doc_id=3665
on 19 May 2006 amending SOLAS. Like AIS, LRIT requires the periodic transmission of the name and position of relevant vessels.

161. Unlike AIS, however, the data will be transmitted only every six hours and such transmissions will take place via satellite directly to an LRIT Data Centre in the flag State. In other words, unlike AIS, LRIT is effectively a closed system. Furthermore, because LRIT transmissions are *via* satellite each LRIT Data Centre is able to track the position of relevant vessels wherever they are.

162. The relevant provisions on LRIT, contained in SOLAS, entered into force on 1 January 2008. The installation of LRIT will be mandatory for the following categories of ships on international voyages constructed on or after 31 December 2008: passenger ships, including high-speed craft; cargo ships, including high-speed craft, of 300 gross tonnage and upwards; and mobile offshore drilling units. A phase-in process is foreseen for vessels built before 31 December 2008.

163. Ships fitted with an AIS and which operate exclusively in Sea Area A1 (in other words within range of shore-based VHF DSC coast stations which is around 40 nm) are exempted from the requirement to fit LRIT.

### 3.3.2 Legal basis

164. The legal basis for LRIT is contained in Chapter V of SOLAS in a new Regulation 19-1 – ‘Long-Range Identification and Tracking of Ships’. In addition Performance Standards and Functional Requirements for the Long Range Identification and Tracking of Ships were adopted by the MSC on 19 May 2006 (the ‘LRIT Performance Standards’).

165. Article 4 of the LRIT Performance standards specifies *inter alia* that LRIT equipment should:

.1 be capable of automatically and without human intervention on board the ship transmitting the ship’s LRIT information at 6-hour intervals to an LRIT Data Centre;
.2 be capable of being configured remotely to transmit LRIT information at variable intervals;
.3 be capable of transmitting LRIT information following receipt of polling commands;
.4 interface directly to the shipborne global navigation satellite system equipment, or have internal positioning capability;
.5 be supplied with energy from the main and emergency source of electrical power.

166. Given that LRIT is a relatively new system, it is not as yet addressed in Community legislation although the European Parliament has proposed that it be included in the VTM Directive as part of the ongoing package of reforms to that text.

167. LRIT was, however, specifically referred to in a Resolution adopted by the Transport Council at its meeting in Luxembourg on 1-2 October 2007 (the Council LRIT Resolution).

### 3.3.3 What data is reported?

168. The data required to be reported pursuant to LRIT is specified in article 5 of Chapter 19-1 of SOLAS. This states:
5 Subject to the provisions of paragraph 4.1, ships shall automatically transmit the following long-range identification and tracking information:

.1 the identity of the ship;

.2 the position of the ship (latitude and longitude); and

.3 the date and time of the position provided.

169. More details are contained in Table 1 of the LRIT Performance Standards as follows.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shipborne equipment identifier</td>
<td>The identifier used by the shipborne equipment.</td>
</tr>
<tr>
<td>Positional data</td>
<td>The GNSS position (latitude and longitude) of the ship (based on the WGS84 datum). Position: The equipment should be capable of transmitting the GNSS position (latitude and longitude) of the ship (based on WGS84 datum) as prescribed by regulation V/19-1, without human interaction on board the ship. On-demand(^{(1)}) position reports: The equipment should be capable of responding to a request to transmit LRIT information on demand without human interaction onboard the ship, irrespective of where the ship is located. Pre-scheduled(^{(2)}) position reports: The equipment should be capable of being remotely configured to transmit LRIT information at intervals ranging from a minimum of 15 min to periods of 6 h to the LRIT Data Centre, irrespective of where the ship is located and without human interaction on board the ship.</td>
</tr>
<tr>
<td>Time Stamp 1</td>
<td>The date and time(^{(3)}) associated with the GNSS position. The equipment should be capable of transmitting the time(^{(3)}) associated with the GNSS position with each transmission of LRIT information.</td>
</tr>
</tbody>
</table>

Notes: \(^{(1)}\) On-demand position reports means transmission of LRIT information as a result of either receipt of polling command or of remote configuration of the equipment so as to transmit at interval other than the preset ones. \(^{(2)}\) Pre-scheduled position reports means transmission of LRIT information at the preset transmit intervals. \(^{(3)}\) All times should be indicated as Universal Co-ordinated Time (UTC).

170. It is, however, necessary to turn to Table 2, which specifies the data to be added by an Application Service Provider and at the LRIT Data Centre in connection with the identity of each participating ship.

171. Table 2 specifies that to the parameter ‘Ship Identity’ are to be added: the IMO ship identification number and the MMSI for the relevant ship.

3.3.4 Why is the data reported?

172. Article 3 of Regulation 19-1 simply states:

This regulation establishes provisions to enable Contracting Governments to undertake the long-range identification and tracking of ships.

173. As Regulation 19-1 is part of SOLAS it seems reasonable to infer that the basic purpose of LRIT is for the safety of navigation. Article 8.1 of the Regulation 19-1 (see next section), however, makes it clear that Contracting Governments shall be
entitled to receive LRIT information for security and other purposes agreed by IMO. These other purposes include maritime security, SAR services\textsuperscript{55} and the protection of the marine environment\textsuperscript{56}.

174. This broader purpose for LRIT is recognised in one of the recitals to the Council Resolution as follows:

Recognizing the added value of managing and organising the sharing of LRIT information within a regional data centre at EU level, for the purposes of maritime security, Search and Rescue (SAR), maritime safety and protection of the marine environment,

\textbf{3.3.5 Who has a right to the data?}

175. Because data is transferred under LRIT in what is effectively a closed system it much easier to regulate who has access to it. This issue is addressed in article 8.1 of the Regulation 19-1. This states:

8.1 Subject to the provisions of paragraphs 8.2 to 11.2, Contracting Governments shall be able to receive long-range identification and tracking information about ships, for security and other purposes as agreed by the Organization, as follows:

.1 the Administration shall be entitled to receive such information about ships entitled to fly its flag irrespective of where such ships may be located;

.2 a Contracting Government shall be entitled to receive such information about ships which have indicated their intention to enter a port facility, as defined in regulation XI-2/1.1.9, or a place under the jurisdiction of that Contracting Government, irrespective of where such ships may be located provided they are not located within the waters landward of the baselines, established in accordance with international law, of another Contracting Government; and

.3 a Contracting Government shall be entitled to receive such information about ships entitled to fly the flag of other Contracting Governments, not intending to enter a port facility or a place under the jurisdiction of that Contracting Government, navigating within a distance not exceeding 1,000 nautical miles of its coast provided such ships are not located within the waters landward of the baselines, established in accordance with international law, of another Contracting Government; and

.4 a Contracting Government shall not be entitled to receive, pursuant to subparagraph .3, such information about a ship located within the territorial sea of the Contracting Government whose flag the ship is entitled to fly.

176. In other words the following, providing they are contracting parties to SOLAS, are entitled to LRIT data:

(a) the flag State at all times;
(b) a port State in respect of a ship that is at sea, irrespective of where it is, that has indicated its intention to enter a port facility in that State or a place under the jurisdiction of that State; and
(c) a coastal State in respect of a ship at sea, other than within the territorial waters of its flag State that is within 1,000 nm of its coast (even if the ship does intend to enter a port in that state).

\textsuperscript{55} MSC.1/Circ.1258 5 June 2008 Guidance to Search and Rescue Services in Relation to Requesting and Receiving LRIT Information

\textsuperscript{56} Resolution MSC.242(83) (adopted on 12 October 2007) use of the long-range identification and tracking information for maritime safety and marine environment protection purposes
177. For reasons of security or other concerns a flag State may determine that LRIT data will not be provided to a coastal State (under scenario (c)) provided notification is provided to the IMO.\textsuperscript{57}

178. In addition, pursuant to Article 12 the SAR services of Contracting Governments to SOLAS are entitled to receive, free of charge, LRIT information in relation to the SAR of persons in distress at sea.

179. As regards the use to which LRIT data is put, Article 10 imposes a duty on Contracting Governments, at all times, to:

.1 recognize the importance of long-range identification and tracking information;

.2 recognize and respect the commercial confidentiality and sensitivity of any long-range identification and tracking information they may receive;

.3 protect the information they may receive from unauthorized access or disclosure; and

.4 use the information they may receive in a manner consistent with international law.

180. Pursuant to Article 11.1 the costs of LRIT information sent and received are to be borne by the Contracting Governments. Specifically, a Contracting Government is not entitled to charge ships that do not fly its flag LRIT transmissions although such charges may be provided for in national legislation in respect of ships flying the flag of such a Contracting Government.

181. Article 8 of the LRIT Performance Standards states that Contracting Governments may establish a National LRIT Data Centre or that they may jointly establish a Regional or Cooperative LRIT Data Centre that may by agreement provide services to other Contracting Governments. In addition, the establishment of an International LRIT Data Centre and International LRIT Data Exchange is foreseen.

182. At the European Community level the Council LRIT Resolution records the Council’s agreement for the establishment of a European Union LRIT Data Centre (EU LRIT DC) to be managed by the Commission in cooperation with the Member States through the European Maritime Safety Agency (EMSA). The objective of the EU LRIT DC is to include maritime security, SAR, maritime safety and protection of the marine environment ‘taking into account respective developments within the IMO context’.

183. The LRIT Resolution further recalls ‘that the LRIT data is owned by the Flag State’ and stresses that ‘the establishment of an EU LRIT DC does not affect the above principle of ownership’.

184. The proposed EU LRIT DC is discussed in more detail below in connection with Safe Sea Net.

\textsuperscript{57} Article 9.1.
3.3.6 Data sharing in practice

185. As LRIT is not yet fully operational LRIT data is not yet shared.

3.4 Ship Reporting Systems

3.4.1 Background

186. A large number of ship reporting systems are currently in place in European Waters. These include: (a) mandatory ship reporting systems that apply to specific stretches of water; (b) a general obligation imposed on the operator, agent or master of a ship bound for a port in a Member State to notify specific information to the port authority; and (c) reporting obligations that apply in respect of specific Vessel Traffic Services. Such schemes, which are considered in more detail below, are typically established to regulate movements in and around ports as well as in particularly congested waters such as the English Channel and the Gulf of Finland.

187. As noted in Regulation 11.1 of Chapter V of SOLAS, ‘Ship reporting systems contribute to safety of life at sea, safety and efficiency of navigation and/or protection of the marine environment’.

188. It is to be noted that such reports are to be filed by radio.

189. The Regulation goes on to note that the IMO ‘is recognized as the only international body for developing guidelines, criteria and regulations on an international level for ship reporting systems’. It provides for reporting systems to be adopted by the IMO on the proposal of Contracting Governments and for the subsequent dissemination of information concerning such systems. However such approval is not necessary for a reporting system to be effective and indeed reporting systems not submitted for IMO approval do not need to comply with Regulation 11.

190. In general terms reporting systems involving more than one Contracting Government are submitted for IMO approval. Nevertheless Regulation 11.3 of Chapter V of SOLAS imposes a duty on Governments establishing ship reporting systems to take into account IMO guidelines and criteria.

191. A ship reporting system, that is adopted and implemented in accordance with IMO guidelines and criteria developed pursuant to Regulation 11, must be used by all ships of certain categories of ships carrying certain cargoes in accordance with the provisions of each system.

192. A series of guidelines and principles have been developed for reporting systems. As regards reporting systems in European Waters, detailed rules are also set out in the VTM Directive. Of these documents Resolution A.851(20) adopted on 27 November 1997 General Principles for Ship Reporting Systems and Ship Reporting Requirements, Including Guidelines for Reporting Incidents involving Dangerous Goods, Harmful Substances and/or Marine Pollutants (Resolution A.851(20)) is of particular relevance concerning the types of information that must be reported.
3.4.2 Port entry

3.4.2.1 Legal Basis

193. Article 4 of the VTM Directive requires the operator, agent or master of a ship bound for a port in a Member State to notify the information specified in Annex 1(1) to the port authority. Such a notification must be made:

- at least 24 hours in advance; or
- at the latest, at the time when the vessel leaves the previous port of departure if the voyage time is less than 24 hours; or
- if the port of call is not known or is changed during the voyage, as soon as this information is available.

194. The term ‘agent’ is defined in Article 3 to mean ‘any person mandated or authorised to supply information on behalf of the operator of the ship’ while ‘port authority’ means ‘the competent authority or body designated by Member States for each port to receive and pass on information reported pursuant to’ the VTM Directive.

195. Furthermore the term ‘ship’ is defined to mean any sea going vessel or craft. However the VTM Directive in general applies to ships of 300 gross tonnage and upwards, unless stated otherwise, but does not apply to:

- warships, naval auxiliaries and other ships owned or operated by a Member State and used for non-commercial public service;
- fishing vessels, traditional ships and recreational craft with a length of less than 45 metres; and
- bunkers below 5,000 tons, ships’ stores and equipment for use on board ships.

3.4.2.2 What data is reported?

196. The data to be reported is specified in Annex I (1) as follows:

(a) ship identification (name, call sign, IMO identification number or MMSI number),

(b) port of destination;

(c) estimated time of arrival at the port of destination or pilot station, as required by the competent authority, and estimated time of departure from that port; and

(d) total number of persons on board.

3.4.3 Mandatory ship reporting systems

197. As already mentioned, a number of mandatory ship reporting systems are to be found in European Waters including GOFREP which applies to the Gulf of Finland, CALDOVEREP which applies to the English Channel and WETREP the West European Tanker Reporting System which was approved by resolution of the IMO MSC on 6 December 2004 (the WETREP Resolution). WETREP, which is an example of an IMO approved mandatory ship reporting system, applies to oil
tankers of more than 600 tonnes deadweight carrying a range of oil products in the Western European Particularly Sensitive Sea Area.  

### 3.4.3.1 Legal Basis

198. Article 9(1) of the VTM Directive states:

The Member State concerned shall monitor and take all necessary and appropriate measures to ensure that all ships entering the area of a mandatory ship reporting system, adopted by the IMO according to Regulation 11 Chapter V of the SOLAS Convention and operated by one or more States, of which at least one is a Member State, in accordance with the relevant guidelines and criteria developed by the IMO, comply with that system in reporting the information required without prejudice to additional information required by a Member State in accordance with IMO Resolution A.851(20).

199. Article 9(2) provides that when a Member State submits a new reporting system to the IMO for adoption (or a proposal to amend an existing system) the information contained in Annex I (4) of the VTM Directive must as a minimum be included.

### 3.4.3.2 What data is reported?

200. Annex I (4) specifies that the following data is to be included in reporting systems submitted to the IMO for adoption:

- **A.** ship identification (name, call sign, IMO identification number or MMSI number),
- **B.** date and time,
- **C. or D.** position in latitude and longitude or true bearing and distance in nautical miles from a clearly identified landmark,
- **E.** course,
- **F.** speed,
- **I.** port destination and estimated time of arrival,
- **P.** cargo and, if dangerous goods present on board, quantity and IMO class,
- **T.** address for the communication of cargo information,
- **W.** total number of persons on board,
- **X.** various information: characteristics and estimated quantity of bunker fuel, for ships carrying more than 5 000 tons of bunker fuel, navigational status.

201. As noted above, Article 9(1) is expressed to be ‘without prejudice to additional information required by a Member State in accordance with IMO Resolution A.851(20)’. The table setting out a standard reporting format includes a longer list of data to be reported as follows:

<table>
<thead>
<tr>
<th>Telegraphy</th>
<th>Telephone (alternative)</th>
<th>Function</th>
<th>Information required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of system (eg AMVER/ AUSREP/ MAREP/ ECAREG/ JASREP)</td>
<td>Name of system (eg AMVER/ AUSREP/ MAREP/ ECAREG/ JASREP State in full)</td>
<td>System identifier</td>
<td>Ship reporting system or nearest appropriate coast radio station</td>
</tr>
<tr>
<td>SP</td>
<td></td>
<td>Sailing plan</td>
<td></td>
</tr>
<tr>
<td>PR</td>
<td></td>
<td>Position report</td>
<td></td>
</tr>
</tbody>
</table>

58 Other mandatory reporting systems in European Waters are (with the responsible Member States indicated in the brackets that follow): ADRIREP (Italy, Slovenia), BONIFREP (France, Italy), CANREP, GIBREP and FINREP (Spain), GBT (GREAT BELT) (Denmark), GDANREP (Poland), OUESSREP (France), TRANSREP (Iceland). EMSA SafeSeaNet monthly report, Ref: F1/Ops/Stats/Apr08, Lisbon April 2008. www.emsa.eu.int/Docs/ssn/ssn_statistics_apr_2008.pdf
<table>
<thead>
<tr>
<th>DR</th>
<th>Deviation report</th>
</tr>
</thead>
<tbody>
<tr>
<td>FR</td>
<td>Final report</td>
</tr>
<tr>
<td>DG</td>
<td>Dangerous goods report</td>
</tr>
<tr>
<td>HS</td>
<td>Harmful substances report</td>
</tr>
<tr>
<td>MP</td>
<td>Marine pollutants report</td>
</tr>
</tbody>
</table>

**Give in full**

Any other report

<table>
<thead>
<tr>
<th>A</th>
<th>Ship (alpha) Ship Name, call sign or ship station identity and flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Time (bravo) Date and time of event</td>
</tr>
<tr>
<td></td>
<td>A 6-digit group giving day of month (first two digits), hours and minutes (last four digits). If other than UTC state time zone used.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>Position (charlie) Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A 4-digit group giving latitude in degrees and minutes suffixed with N (north) or S (south) and a 5-digit group giving longitude in degrees and minutes suffixed with E (east) or W (west); or</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
<th>Position (delta) Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>True bearing (first 3 digits) and distance (state distance) in nautical miles from a clearly identified landmark (state landmark)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
<th>Course (echo) True course</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A 3-digit group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F</th>
<th>Speed (foxtrot) Speed in knots and tenths of knots</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A 3-digit group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G</th>
<th>Departed (golf) Port of departure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of last port of call</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H</th>
<th>Entry (hotel) Date, time and point of entry into system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Entry time expressed as in (B) and entry position expressed as in (C) or (D)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
<th>Destination and ETA (India) Destination and time of expected arrival</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of port and date time group expressed in (B)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J</th>
<th>Pilot (juliet) Pilot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>State whether a deep-sea or local pilot is on board</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K</th>
<th>Exit (kilo) Date, time and point of exit from system or arrival at the ship's destination</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exit time expressed as in (B) and exit position expressed as in (C) or (D)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L</th>
<th>Route (lima) Route information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Intended track</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>Radiocommunication (mike) Radiocommunications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>State in full names of stations/frequencies guarded</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N</th>
<th>Next report (november) Time of next report</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date time group expressed as in (B)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>O</th>
<th>Draught (oscar) Maximum present static draught in metres</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4-digit group giving metres and centimetres</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P</th>
<th>Cargo Cargo on board</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cargo and brief details of any dangerous harmful substances and gases that could endanger persons or the environment (See detailed reporting requirements)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q</th>
<th>Defect, damage, deficiency, limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Defects/damage/Deficiencies/other</td>
</tr>
<tr>
<td></td>
<td>Brief details of defects, damage, deficiencies or</td>
</tr>
</tbody>
</table>

40
<table>
<thead>
<tr>
<th>(quebec)</th>
<th>Limitations</th>
<th>other limitations (See detailed reporting requirements)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Pollution/dangerous goods lost overboard (romeo)</td>
<td>Description of pollution or dangerous goods lost overboard</td>
</tr>
<tr>
<td>S</td>
<td>Weather (sierra)</td>
<td>Weather conditions</td>
</tr>
<tr>
<td>T</td>
<td>Agent (tango)</td>
<td>Ship’s representative and/or owner</td>
</tr>
<tr>
<td>U</td>
<td>Size and type (uniform)</td>
<td>Ship size and type</td>
</tr>
<tr>
<td>V</td>
<td>Medic (victor)</td>
<td>Medical personnel</td>
</tr>
<tr>
<td>W</td>
<td>Persons (whiskey)</td>
<td>Total number of persons on board</td>
</tr>
<tr>
<td>X</td>
<td>Remarks</td>
<td>Miscellaneous</td>
</tr>
<tr>
<td>Y</td>
<td>Relay (yankee)</td>
<td>Request to relay report to another system - eg AMVER, AUSREP, JASREP, MAREP etc</td>
</tr>
<tr>
<td>Z</td>
<td>End of report (zulu)</td>
<td>End of report</td>
</tr>
</tbody>
</table>

202. To take an actually example of a reporting system, the WETREP reporting requirements must contain the following information:

.1 the ship’s name, call sign, IMO number/MMSI number and position are needed for establishing the identity of the ship and its initial position (letters A, B and C);  
.2 the ship’s course, speed and destination, are important in order to maintain track of the ship so as to be able to implement search and rescue measures if a report from a ship fails to appear; to be able to instigate measures for the safe navigation of the ship; and to prevent pollution in the areas where weather conditions are severe (letters E, F, G and I ). Proprietary information obtained as a requirement of the mandatory ship reporting system WETREP will be protected under this system consistent with the Guidelines and Criteria for Ship Reporting Systems, as amended (resolution A.851(20));  
.3 the number of persons on board and other relevant information are important in relation to the allocation of resources in a search and rescue operation (letters P, T and W); and  
.4 in accordance with the provisions of the SOLAS and MARPOL conventions, ships will provide information on defects, damage, deficiencies or other limitations (under “Q”) as well as, additional information (under “X”).

203. Specific rules specify when reports must be submitted (eg on entry into and exit from the specified Reporting Area, which is also described in the WETREP Resolution, as well as route deviations).
204. Regulation 3.4.3 specifies that ‘Reports may be sent by any modern communication form including Inmarsat-C, telefax and e-mail as appropriate’.

3.4.4 Why is the data reported?

205. As regards mandatory ship reporting systems the main reasons why these are established are: (a) to promote the safety of navigation and the prevention of accidents; and (b) in the event of an incident to enable the responsible authorities to respond effectively so as to provide rescue services and to minimise or prevent pollution.

206. The objectives of WETREP, for example, are specified to be to ‘initiate SAR and measures to prevent pollution as fast and effectively as possible if an emergency is reported or a ship fails to appear and it is impossible to establish communication with the ship’.

3.4.5 Who has a right to the data?

207. As regards port entry reporting requirements, Article 4 if the VTM Directive, as already described, specifies that the data is to be sent to the relevant port authority.

208. Because each reporting system is unique it will specify precisely to whom the information is to be transmitted. In the case of WETREP for example the list of ‘vessel traffic services, RCC, coast radio station or other facilities’ to whom reports must be submitted are listed in Appendix 1 to the relevant MSC Resolution approving the System. In fact these are all Marine Rescue Coordination Centres (MRCCs).

3.5 Notification of Dangerous or Polluting Goods on Board Ships (Hazmat)

3.5.1 Background

209. The Hazmat reporting requirements are contained in Title II of the VTM Directive. In outline, the Directive requires the prior notification of the presence of dangerous or polluting goods carried on vessels: (a) departing from a port in a Member State; or (b) coming from a port outside the Community and bound for a port in a Member State or an anchorage located in the territorial waters of a Member State.

210. These requirements substantially reproduce and update the provisions of Council Directive 93/75/EEC of 13 September 1993 concerning minimum requirements for vessels bound for or leaving Community ports and carrying dangerous or polluting goods (the Hazmat Directive) which was repealed by the VTM Directive.

211. The recital to the Hazmat Directive refers both to SOLAS and another IMO sponsored convention the International Convention for the Prevention of Pollution
from Ships, 1973, as modified by the Protocol of 1978 relating thereto (MARPOL 73/78). MARPOL is the principal international convention addressing the prevention of pollution of the marine environment by ships from operational or accidental causes.

212. Essentially the Hazmat reporting regime is but another form of ship reporting system and its overall format follows that specified in Resolution A.851(20) (described in section 3.4.1 above).

3.5.2 Legal basis

213. As already stated, the legal basis for Hazmat is contained in Title II of the VTM Directive which contains four articles, articles 12-15. Article 12 is not relevant to this discussion.

214. Article 13(1) concerns the obligation to notify to the relevant competent authority the presence of dangerous or hazardous goods prior to departure from a port of a Member State. Article 13(2) is concerned with the ships coming from a port outside the Community, carrying dangerous or polluting goods and bound for a port in a Member State or an anchorage located in the territorial waters of a Member State. It states:

The operator, agent or master of a ship, irrespective of its size, carrying dangerous or polluting goods coming from a port located outside the Community and bound for a port of a Member State or an anchorage located in a Member State's territorial waters shall, at the latest upon departure from the loading port or as soon as the port of destination or the location of the anchorage is known, if this information is unavailable at the moment of departure, notify the information indicated in Annex I(3) to the competent authority of the Member State in which the first port of destination or anchorage is located.

215. Article 13(3) provides that the Member States may put into place a procedure authorising the operator, agent or master of a ship referred to in paragraphs (1) or (2) to make a notification to the port authority of the port of departure or the port of destination in the Community as appropriate. The data that must be contained in each notification is set out in Annex I (3) of the VTM Directive.

216. Article 13(3) continues:

The procedure put in place must ensure that the competent authority has access to the information indicated in Annex I(3) at all times should it be needed. To this end, the port authority concerned shall retain the information listed in Annex I(3) long enough for it to be usable in the event of an incident or accident at sea. The port authority shall take the necessary measures to provide this information electronically and without delay to the competent authority, 24 hours a day upon request.

217. Article 14 goes on to require the Member States to cooperate to ensure the interconnection and inter-operability of the national systems used to manage all of the information indicated in Annex I, including the Hazmat data. Communications systems set in fulfilment of this obligation must:

- provide for the electronic exchange of data and enable messages notified in accordance with Article 13 to be received and processed;
- enable information to be transmitted 24 hours a day; and
enable each Member State, upon request, to send information on the ship and the dangerous or polluting goods on board without delay to the competent authority of another Member State.

218. These provisions are considered in greater detail below in connection with SafeSeaNet.

219. Finally a number of exemptions are provided for in Article 14 in respect of scheduled services provided various procedures are followed including as regards the retention of data.

3.5.3 What data is reported?

220. The data that must be reported is specified in Article 13 (3) by reference to Annex I (3) of the VTM Directive. Annex I (3) states:

Information to be notified in accordance with Article 13:

A. General information:
   (a) ship identification (name, call sign, IMO identification number or MMSI number);
   (b) port of destination;
   (c) for a ship leaving a port in a Member State: estimated time of departure from the port of departure or pilot station, as required by the competent authority, and estimated time of arrival at the port of destination;
   (d) for a ship coming from a port located outside the Community and bound for a port in a Member State: estimated time of arrival at the port of destination or pilot station, as required by the competent authority;
   (e) total number of persons on board.

B. Cargo information:

   (a) the correct technical names of the dangerous or polluting goods, the United Nations (UN) numbers where they exist, the IMO hazard classes in accordance with the IMDG, IBC and IGC Codes and, where appropriate, the class of the ship as defined by the INF Code, the quantities of such goods and their location on board and, if they are being carried in cargo transport units other than tanks, the identification number thereof;
   (b) confirmation that a list or manifest or appropriate loading plan giving details of the dangerous or polluting goods carried and of their location on the ship is on board;
   (c) address from which detailed information on the cargo may be obtained.

221. ‘Dangerous goods’ are described in article 1 of the VTM Directive to mean:

- goods classified in the IMDG Code,
- dangerous liquid substances listed in Chapter 17 of the IBC Code,
- liquefied gases listed in Chapter 19 of the IGC Code,
- solids referred to in Appendix B of the BC Code.

Also included are goods for the carriage of which appropriate preconditions have been laid down in accordance with paragraph 1.1.3 of the IBC Code or paragraph 1.1.6 of the IGC Code;

222. The IMDG, IBC and IGC Codes are respectively the International Maritime Dangerous Goods Code, the International Code for the Construction and Equipment of Ships Carrying Dangerous Chemicals in Bulk and the International Gas Carriers’ Code.

223. ‘Polluting goods’ are described in article 1 of the VTM Directive as:

i. oils as defined in Annex I to the MARPOL Convention,
ii. noxious liquid substances as defined in Annex II to the MARPOL Convention,
iii. harmful substances as defined in Annex III to the MARPOL Convention;
3.5.4 Why is the data reported?

224. The reasons why this data is reported can best be determined by reference to the purpose of the VTM Directive which is set out in Article 1 as follows:

The purpose of this Directive is to establish in the Community a vessel traffic monitoring and information system with a view to enhancing the safety and efficiency of maritime traffic, improving the response of authorities to incidents, accidents or potentially dangerous situations at sea, including search and rescue operations, and contributing to a better prevention and detection of pollution by ships.

3.5.5 Who has a right to the data?

225. In connection with the specific Hazmat provision the persons who are entitled to receive hazmat data are:

(a) the competent authority designated by a Member State prior to the departure from a port within that Member State of a vessel carrying dangerous or polluting goods;
(b) the competent authority designated by a Member State prior to the arrival in a port of that Member State, or an anchorage located within the territorial waters of that Member State, in the case of a vessel carrying dangerous or polluting goods coming from a port outside the Community.

3.6 Incident and accident reporting requirements

3.6.1 Background

226. Title III of the VTM Directive establishes a number of reporting requirements concerning incidents and accidents at sea. More specifically the directive requires the Member States to monitor and to ‘take appropriate measures to ensure that the master of a ship sailing within their SAR region or EEZ or equivalent immediately notifies the coastal station responsible for the geographical area regarding a number of incidents and accidents’.

227. This obligation is in addition to a general duty that is imposed by SOLAS on the master of every ship that meets a number of ‘dangerous conditions’ to communicate the information by all means at his disposal to ships in the vicinity, and also to the competent authorities.

3.6.2 Legal basis

59 Mention can also be made to Article 12 of the VTM Directive which imposes a duty on the shipper of dangerous or polluting goods to deliver a declaration to the master or operator of a ship before such goods are offered for carriage or taken on board. The contents of such a declaration of cargo information are specified in Annex I (2).
The legal basis for the first obligation is provided by Article 17 (1) of the VTM Directive.

The legal basis of the general duty to report ‘dangerous conditions’ is imposed by Regulation 31 of Chapter V of SOLAS.

3.6.3 What data is reported?

The incidents and accidents that must be reported pursuant to Article 17(1) of the VTM Directive are:

(a) any incident or accident affecting the safety of the ship, such as collision, running aground, damage, malfunction or breakdown, flooding or shifting of cargo, any defects in the hull or structural failure;

(b) any incident or accident which compromises shipping safety, such as failures likely to affect the ship's manoeuvrability or seaworthiness, or any defects affecting the propulsion system or steering gear, the electrical generating system, navigation equipment or communications equipment;

(c) any situation liable to lead to pollution of the waters or shore of a Member State, such as the discharge or threat of discharge of polluting products into the sea;

(d) any slick of polluting materials and containers or packages seen drifting at sea.

In addition, Article 17(2) goes on to provide that the ‘report message’ sent in application of paragraph 1 must include specified data about the ship from which the report is made. This data must ‘include at least the ship’s identity, its position, the port of departure, the port of destination, the address from which information may be obtained on the dangerous and polluting goods carried on board, the number of persons aboard, details of the incident and any relevant information referred to in IMO Resolution A.851(20)’.

The dangerous conditions that must reported pursuant to SOLAS, Chapter V, Regulation 31 include ‘dangerous ice, a dangerous derelict, or any other direct danger to navigation, or a tropical storm, or encounters sub-freezing air temperatures associated with gale force winds causing severe ice accretion on superstructures, or winds of force 10 or above on the Beaufort scale for which no storm warning has been received’. There is no mandatory format in which the information contained in such ‘danger messages’ must be sent. Such information can be transmitted either in plain language (preferably English) or by means of the International Code of Signals.

3.6.4 Why is the data reported?

Article 17 (1) of the VTM Directive specifically states that the purpose for which the data is to be reported is ‘with a view to preventing or mitigating any significant threat to maritime safety, the safety of individuals or the environment’.

3.6.5 Who has a right to the data?

Although Article 17(1) of the VTM Directive requires the master of a ship to immediately report specified incidents and accidents to the relevant coastal station,
Article 21 goes on to provide for the onward transmission of such data. Specifically Article 21(1) states:

The competent coastal station of the Member States concerned shall, as necessary, broadcast within the relevant areas any incident or accident notified under Article 17(1) and information with regard to any ship that poses a threat to maritime safety, the safety of individuals or the environment.

235. Furthermore, competent authorities holding data notified in accordance with Article 13 of the VTM Directive (Hazmat reporting data) as well as data notified pursuant to Article 17 are required by Article 21(2) to make ‘adequate arrangements to provide such information at any time upon request for safety reasons by the competent authority of another Member State’.

236. Thereafter, article 22(3) provides that:

Any Member State the competent authorities of which have been informed, pursuant to this Directive or in some other way, of facts which involve or increase the risk for another Member State of a hazard being posed to certain shipping areas and coastal zones, shall take the appropriate measures to inform any interested Member State thereof as soon as possible and consult it regarding the action being envisaged. Where appropriate, Member States shall cooperate with a view to pooling the arrangements for joint action.

Each Member State shall make the necessary arrangements to use fully the reports which ships are required to transmit to them pursuant to Article 17.

237. With regard to the danger messages sent pursuant to Chapter V of SOLAS, Regulation 31.2 requires each Contracting Government to ‘take all steps necessary to ensure that when intelligence of any of the dangers specified in paragraph 1 is received, it will be promptly brought to the knowledge of those concerned and communicated to other interested Governments’.

3.7 Port Security Notification Requirements – Regulation 725/2004 (EC)

3.7.1 Background and legal basis


239. The Port Security Regulation also seeks to provide a basis for the harmonised interpretation, implementation and Community monitoring of ‘the special measures to enhance maritime security adopted by the Diplomatic Conference of the IMO on 12 December 2002’.

240. These measures comprised the amendment of SOLAS, through the inclusion of a new Chapter XI-2, as well as the adoption of the International Ship and Port Facility Security Code (ISPS Code). Copies of the new Chapter XI-2 of SOLAS and the ISPS Code are both annexed to the Port Security Regulation (as Annexes I and II respectively).

60 Article 1(1).
241. In outline, the new Chapter XI-2 of SOLAS requires Contracting Governments to establish security levels for relevant ships entitled to fly their flag and port facilities within their territory and to provide security level information to such vessels, port facilities and to relevant ships entering those ports. The term ‘security level’ is defined to mean ‘the qualification of the degree of risk that a security incident will be attempted or will occur’. Chapter XI-2 applies to specified types of ship engaged on international voyages (namely passenger ships including high speed passenger craft, cargo ships including high speed craft, of 500 gross tonnage and upwards and mobile offshore drilling units) and port facilities serving such ships on international voyages.

242. Thereafter, ships and shipping companies are required to comply with the relevant provisions of Chapter XI-2 and the ISPS code. To this end each ship must, before entering a port within the territory of Contracting Government (or while present in such a port), comply with the requirements of the applicable security level and must respond without delay to any change to a higher security level.

243. Chapter XI-2 also requires the installation of ship security alert systems in accordance with a specified timetable. Such systems must, when activated, send a secret security alert to the competent authority specified by the Administration of the Contracting Government that must identify the ship, its location and the fact that the ship’s security is under threat or has been compromised. Such an alert must not raise the alarm on board the vessel itself or be transmitted to other vessels.

244. Other provisions inter alia concern the procedures for the setting of security levels, address the exercise of discretion by the masters of vessels, establish requirements for port facilities, and specify the procedures for the communication of information between Contracting Governments and the IMO.

245. Of relevance to this Study are the control and compliance measures foreseen in Regulation 9 and, in particular, the provisions of that article which address the duties of ships intending to enter a port of a Contracting Government. Regulation 9.2.1 states:

2.1 For the purpose of this chapter, a Contracting Government may require that ships intending to enter its ports provide the following information to officers duly authorised by that Government to ensure compliance with this chapter prior to entry into port with the aim of avoiding the need to impose control measures or steps:

.1 that the ship possesses a valid Certificate and the name of its issuing authority;

.2 the security level at which the ship is currently operating;

.3 the security level at which the ship operated in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.4 any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within the timeframe specified in paragraph 2.3;

.5 that the appropriate ship security procedures were maintained during any ship to ship activity within the timeframe specified in paragraph 2.3; or

---

61 Regulation 3.
62 Regulation 1.14.
63 Regulation 6.
.6 other practical security related information (but not details of the ship security plan), taking into account the guidance given in part B of the ISPS Code.

If requested by the Contracting Government, the ship or the Company shall provide confirmation, acceptable to that Contracting Government, of the information required above.

246. Paragraph 2.3 requires ships to maintain records of information of this type for the last 10 calls at port facilities. If a Master fails to provide such information, entry into port may be denied.

247. Further provisions go on to address measures that the port State officials may undertake in order to rectify non-compliance with the requirements of Chapter XI-2 and the ISPS Code. The guidance given in Part B of the ISPS Code refers to paragraphs 4.37 and 4.38.

248. Paragraph 4.37 states:

4.37 Regulation XI-2/9.2.1 lists the information Contracting Governments may require from a ship as a condition of entry into port. One item of information listed is confirmation of any special or additional measures taken by the ship during its last 10 calls at a port facility. Examples could include:

.1 records of the measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government, especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments; and

.2 any Declarations of Security that were entered into with port facilities or other ships.

249. Paragraph 4.38 provides as follows:

4.38 Another item of information listed, that may be required as a condition of entry into port, is confirmation that appropriate ship security procedures were maintained during ship-to-ship activity conducted within the period of the last 10 calls at a port facility. It would not normally be required to include records of transfers of pilots or of customs, immigration or security officials nor bunkering, lightering, loading of supplies and unloading of waste by ship within port facilities as these would normally fall within the auspices of the PFSP. Examples of information that might be given include:

.1 records of the measures taken while engaged in a ship-to-ship activity with a ship flying the flag of a State which is not a Contracting Government, especially those measures that would normally have been provided by ships flying the flag of Contracting Governments;

.2 records of the measures taken while engaged in a ship-to-ship activity with a ship that is flying the flag of a Contracting Government but is not required to comply with the provisions of chapter XI-2 and part A of this Code, such as a copy of any security certificate issued to that ship under other provisions; and

.3 in the event that persons or goods rescued at sea are on board, all known information about such persons or goods, including their identities when known and the results of any checks run on behalf of the ship to establish the security status of those rescued. It is not the intention of chapter XI-2 or part A of this Code to delay or prevent the delivery of those in distress at sea to a place of safety. It is the sole intention of chapter XI-2 and part A of this Code to provide States with enough appropriate information to maintain their security integrity.

4.39 Examples of other practical security-related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:

.1 information contained in the Continuous Synopsis Record;

.2 location of the ship at the time the report is made;

.3 expected time of arrival of the ship in port;
4. crew list;
5. general description of cargo aboard the ship;
6. passenger list; and
7. information required to be carried under regulation XI-2/5.

250. Furthermore, in accordance with Paragraph 4.41:

4.41 In all cases where a ship is denied entry or is expelled from a port, all known facts should be communicated to the authorities of relevant States. This communication should consist of the following, when known:

1. name of ship, its flag, the Ship Identification Number, call sign, ship type and cargo;
2. reason for denying entry or for expulsion from port or port areas;
3. if relevant, the nature of any security non-compliance;
4. if relevant, details of any attempts made to rectify any non-compliance, including any conditions imposed on the ship for the voyage;
5. past port(s) of call and next declared port of call;
6. time of departure and likely estimated time of arrival at those ports;
7. any instructions given to the ship, e.g., reporting on its route;
8. available information on the security level at which the ship is currently operating;
9. information regarding any communications the port State has had with the Administration;
10. contact point within the port State making the report for the purpose of obtaining further information;
11. crew list; and
12. any other relevant information.

251. The next paragraph provides that ‘relevant States’ could include States on the ship’s passage to its next port as well as previous courts of call.

252. Returning to the provisions of the Port Security Regulation, Article 6 provides that the competent authority for maritime security of a Member State shall require the information referred to paragraph 2.1 of regulation 9 (of SOLAS Chapter XI-2) to be provided by any vessel subject to SOLAS, Chapter XI-2, the ISPS Code or Article 3 of the Port Security Regulation that announces its intention to enter a port of that Member State.

253. Such information must be provided at least 24 hours in advance or at the latest at the time when the ship leaves the previous port if the voyage time is less than 24 hours or, if the port of call is not known or if there is a change of plan, as soon as the port of call is known.64

64 Article 7(3).
254. Provision is made in Article 7 for the exemption from these reporting requirements of scheduled services provided certain specified requirements are complied with.

3.7.2 What data is reported?

255. Further guidance as to the type and form of the data to be transmitted is contained in Chapter 3 of the Guidance Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code issued by IMO MSC on 7 June 2004 (the ‘ISPS Guidance’). A copy of the ISPS Guidance is attached as Annex R.

3.1 The Contracting Government may, in ensuring compliance with chapter XI-2, require that ships intending to enter its ports provide the following information (regulation XI-2/9.2.1):

.1 confirmation that the ship possesses a valid ISSC or a valid Interim ISSC and the name of its issuing authority (regulation XI-2/9.2.1.1);

.2 the security level at which the ship is currently operating (regulation XI 2/9.2.1.2);

.3 the security level at which the ship operated in the previous ten calls at port facilities (regulation XI-2/9.2.1.3);

.4 any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship/port interface within the timeframe specified paragraph 3.1.3 above (regulation XI-2/9.2.1.4). For example, a ship may provide, or be requested to provide, information that might be recorded in the ship's log book or in another document such as the ship's security log book, related to:

.1 measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government, especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments (ISPS Code paragraph B/4.37.1); and

.2 any Declarations of Security that were entered into with port facilities or other ships (ISPS Code paragraph B/4.37.2);

.5 confirmation that appropriate ship security procedures were maintained during any ship-to-ship activity during the period covered by its previous ten calls at port facilities (regulation XI-2/9.2.1.5). For example, a ship may provide, or be requested to provide, information related to:

.1 measures taken while engaged in a ship-to-ship activity with a ship flying the flag of a State which is not a Contracting Government, especially those measures that would normally have been provided by ships flying the flag of Contracting Governments (ISPS Code paragraph B/4.38.1);

.2 measures taken while engaged in a ship-to-ship activity with a ship flying the flag of a Contracting Government but not required to comply with the provisions of chapter XI-2 and part A of the ISPS Code, such as a copy of any security certificate issued to that ship under other provisions (ISPS Code paragraph B/4.38.2); and

.3 in the event that persons or goods rescued at sea are on board, all known information about such persons or goods, including their identities when known and the results of any checks run on behalf of the ship to establish the security status of those rescued. It is not the intention of chapter XI-2 or part A of the ISPS Code to delay or prevent the delivery of those in distress at sea to a place of safety. It is the sole intention of chapter XI-2 and part A of the ISPS Code to provide States with enough appropriate information to maintain their security integrity (ISPS Code paragraph B/4.38.3);

.6 other practical security related information (but not details of the ship security plan) (regulation XI-2/9.2.1.6). For example, a ship may provide, or be requested to provide, information related to:
information contained in the Continuous Synopsis Record (CSR) (ISPS Code paragraph B/4.39.1);
.2 location of the ship at the time the report is made (ISPS Code paragraph B/4.39.2);
.3 expected time of arrival of the ship in port (ISPS Code paragraph B/4.39.3);
.4 crew list6 (ISPS Code paragraph B/4.39.4);
.5 general description of cargo aboard the ship7 (ISPS Code paragraph B/4.39.5);
.6 passenger list8 (ISPS Code paragraph B/4.39.6);
.7 information regarding who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship (ISPS Code paragraph B/4.39.7 and regulation XI-2/5);
.8 information regarding who is responsible for deciding the employment of the ship (ISPS Code paragraph B/4.39.7 and regulation XI-2/5); and
.9 in cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies). (ISPS Code paragraph B/4.39.7 and regulation XI-2/5).

256. Footnotes 6-8 list: the IMO Crew List; IMO FAL Form 5; the IMO Cargo Declaration; IMO FAL Form 2; the IMO Passenger List, and IMO FAL Form 6 respectively.

257. The reference ‘FAL’ is an abbreviated term used to describe the IMO sponsored ‘Convention on Facilitation of International Maritime Traffic’ 1965 as most recently amended in 2005 (‘the FAL Convention’).

258. The main purpose of the FAL Convention is to prevent unnecessary delays in maritime traffic, to aid co-operation between Governments and to secure the highest practicable degree of uniformity in formalities and other procedures by reducing to just eight the number of declarations which can be required by public authorities in respect port arrivals, stays and departures.

259. One feature of the FAL Convention is its use of binding ‘Standards’ which are defined as internationally-agreed measures which are “necessary and practicable in order to facilitate international maritime traffic” and ‘recommended practices’ as measures the application of which is “desirable”.

### 3.7.3 Why is the data reported?

260. Given the slightly convoluted manner in which the Port Security Regulation reporting requirements are imposed, the regulation itself does not contain a clear statement as to the purpose of the reporting requirement. Instead it is necessary to infer this from the overall purpose of the Port Security Regulation as set out in Article 1(1) as described above.

### 3.7.4 Who has a right to the data?

261. The competent authority for maritime security, which is defined in Article 2(7) as:

an authority designated by a Member State to coordinate, implement and monitor the application of the security measures laid down in this Regulation in respect of ships and/or one or more port facilities. The competences of this authority may differ depending on the tasks assigned to it.
3.8 Schengen notification requirements

3.8.1 Background and legal basis


263. Apart from providing for the absence of border control of persons crossing the ‘internal borders’ of the European Union, the Schengen Borders Code also ‘establishes rules governing border control of persons crossing the external borders of the Member States of the European Union’.65 In fact the Schengen Borders Code develops aspects of the Schengen acquis in which Ireland and the United Kingdom do not participate. Consequently the Code does not apply to them and the notions of the EU’s internal and external borders must be understood to include only the Member States within the ‘Schengen Area’ (i.e. not including Ireland and the United Kingdom).

264. The scope of the Schengen Borders Code goes far beyond notification requirements. It contains inter alia detailed provisions on border crossings, entry conditions for third country nationals, the control of external borders including the conduct of border checks, the stamping of travel documents and border surveillance, the resources necessary for border control and cooperation between Member States.

3.8.2 What data is reported?

265. Annex VI contains specific rules for various types of borders and the crossing of the Member States’ external borders including ‘sea borders’. The term ‘external borders’ is defined in Article 2(2) to mean ‘Member States’ land borders, including river and lake borders, sea borders and their airports, river ports, sea ports and lake ports, provided that they are not internal borders’.

266. The term ‘internal borders’ is described to mean inter alia ‘sea, river and lake ports of the Member States for regular ferry connections’.

267. As regards the crossing of sea borders, Article 3.1.2 of Annex VI imposes a duty on the ship’s captain or, failing that, the individual or corporation who represents the shipowner in all matters relating to the shipowner's duties in fitting out the vessel (shipowner's agent), to draw up a list, in duplicate, of the crew and of any passengers. This list must, at the latest upon the ship’s arrival in port, be given to the border guards. If, for reasons of force majeure, the list or lists cannot be sent to the border guards, a copy must be sent to the appropriate border post or shipping authority, which must in turn forward it without delay to the border guards.

65 Article 1.
268. Thereafter, one copy of the two lists, duly signed by the border guards, must be returned to the ship's captain, who is required to produce it on request when in port. Any changes to the composition of the crew or the number of passengers must be promptly notified to the competent authority by the ship’s captain or failing that by the shipowner’s agent. Furthermore, the captain must notify the competent authority promptly, and if possible, even before the ship enters port, of the presence on board of stowaways. Such stowaways will, however, remain under the responsibility of the ship's captain.

269. Before the ship’s departure, the captain is required to notify the border guards in due time and in accordance with the rules in force in the port concerned; if he or she is unable to notify them, he or she must advise the appropriate shipping authority. The second copy of the previously completed and signed list(s) must then be returned to the border guards or shipping authorities. No specific format is specified for such lists.

270. In accordance with Annex VII, special rules are established for certain categories of persons including seamen.

271. Article 3(1) provides that, by way of derogation from Articles 4 and 7, ‘Member States may authorise seamen holding a seafarer's identity document issued in accordance with the Geneva Convention of 19 June 2003 (No 185), the London Convention of 9 April 1965 and the relevant national law, to enter into the territory of the Member States by going ashore to stay in the area of the port where their ships call or in the adjacent municipalities without presenting themselves at a border crossing point, on condition that they appear on the crew list, which has previously been submitted for checking by the competent authorities, of the ship to which they belong’.

272. However, according to the assessment of the risks of internal security and illegal immigration, seamen shall be subject to a check in accordance with Article 7 by the border guards before they go ashore. If a seaman constitutes a threat to public policy, internal security or public health, he may be refused permission to go ashore. However, seamen who intend to stay outside the municipalities situated in the vicinity of ports must comply with the general conditions for entry by third country national into to the territory of the Member States, as set out in Article 5(1).

273. In addition some specific procedures are provided for in respect of certain types of shipping, some of which involve prior notification requirements.

274. As regards ‘cruise ships’, which are defined to mean ships that follow ‘a given itinerary in accordance with a predetermined programme, which includes a programme of tourist activities in the various ports, and which normally neither takes passengers on nor allows passengers to disembark during the voyage’, the itinerary and programme of the cruise must be notified to the border guards at least 24 hours before the ship leaves the port of departure and before its subsequent arrival in each port in the territory of the Member States.
275. Provided the itinerary comprises exclusively ports located within the Member States, no border checks are undertaken unless this is considered necessary following an assessment of the risks relating to internal security and illegal immigration. If, however, the itinerary of a cruise ship comprises both ports situated in the territory of the Member States and ports situated in third countries, a modified procedure for border checks is specified under which, based on a risk assessment, such checks may in some circumstances be dispensed with.

276. A central role in this modified procedure is played by ‘nominal lists’ of passengers and crew. Pursuant to Article 3.24 these must include:

(a) name and surname;
(b) date of birth;
(c) nationality;
(d) number and type of travel document and, where applicable, visa number.

277. Nominal lists must be transmitted by the ship’s captain or, failing that, by the owner’s agent to the relevant border guards at least 24 hours before the arrival at each port in the territory of the Member States or, where the journey to this port lasts less than 24 hours, immediately after the boarding is completed in the previous port. The nominal list must be stamped at the first port of entry into the territory of the Member States of following any modification to its contents.

278. In the case of pleasure boats, persons on board a pleasure boat coming from, or departing, a port situated in a Member State are subject to border checks and may enter a port which is not a border crossing point. However checks and/or physical searches of pleasure boats are to be undertaken following an assessment of the risks of illegal immigration and, in particular, where the coastline of a third country is located in the immediate vicinity of the territory of the Member State concerned. The term 'pleasure boating' is defined to mean 'the use of pleasure boats for sporting or tourism purposes.\textsuperscript{66}

279. Furthermore, by way of exception to Article 4, which requires external borders to be crossed only at border crossing points (and during fixed opening hours), a pleasure boat coming from a third country may enter a port which is not a border crossing point provided the relevant port authorities are notified. The port authorities must, in turn, contact the authorities in the nearest port designated as a border crossing point in order to report the vessel's arrival. The declaration regarding passengers must be be made by lodging the list of persons on board with the port authorities. That list must be made available to the border guards, at the latest upon arrival. Similar provisions apply in cases where a pleasure boat coming from a third country has to dock for reasons of force majeure.

280. During such checks, a document containing the technical characteristics of the vessel and the names of the persons on board must be handed in. A copy of that document must be given to the authorities in the ports of entry and departure. As long as the vessel remains in the territorial waters of one of the Member States, a copy of that document must be included amongst the ship's papers.

\textsuperscript{66} Article 2(17).
281. A further relaxation of the standard procedure is made for the crews of coastal fisheries vessels (vessels which return every day, or within 36 hours, to a port situated in the territory of a Member State without calling at a port situated in a third country) who are not subject to systematic border checking. Crews of coastal fisheries vessels from outside the Schengen Area are to be checked, though, in accordance with the provisions applicable to seamen.

3.8.3 Why is the data reported?

282. The data is reported in order to facilitate the undertaking of border checks in order to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it.

3.8.4 Who has a right to the data?

283. The data must be supplied to the border guards of the border that is intended to be crossed. Article 16, however, which is entitled ‘Cooperation between Member States’ provides that the Member States must ‘assist each other’ and must ‘maintain close and constant cooperation with a view to the effective implementation of border control…’. The article goes on to provide that they ‘shall exchange all relevant information’. 
4 Surveillance systems

284. Under this heading are included systems under which data is gathered by surveillance methods in respect of which the person who is subject to the scheme plays no active part. The main limitations of such ‘non-cooperative’ systems lies in the fact that only limited information can be provided by what is essentially a visual image albeit one that may be treated or conveyed to a video screen. The nature of the image and the data that can represent such an image have important implications as regards data processing and management.

285. The types of image, and thus data, that can be acquired will depend on the particular technique used. Visual sightings, whether direct or through binoculars or transferred to a remote location by camera, may provide details of the name and the IMO number of a vessel. The size and type of the vessel can be identified along with an assessment of its course and speed. A radar image or infra-red image may provide information only that there is a vessel present and an idea of its course and speed.

286. At the same time, notwithstanding the relevant lack of detail that can be obtained from purely surveillance techniques, non-cooperative surveillance systems have an important role to play in building up a compiled maritime picture.

287. First of all, a vessel may fail to provide the information required by a relevant reporting regime. This may be for an innocent reason, such as the failure of equipment. Or it may be deliberate through, for example, the deactivation of a VMS transponder or AIS transmitter. In such circumstances, the surveillance system may provide the only means of determining the presence or otherwise of a vessel. Second, existing reporting regimes may not apply to certain types of vessel due, for example, to their small size. Third, radar and visual systems may be more accurate in terms of spatial location, more immediate and more responsive than computer or satellite-based systems.

288. Surveillance is undertaken within coastal waters and on the high seas for a wide range of different reasons. For the purpose of analysis it is convenient to break these reasons down into two main categories: military and non-military. Beyond these main distinctions, a number of specific systems referred to in the terms of reference are considered.

4.1 Military surveillance systems

4.1.1 Background and legal basis

289. The acquisition of surveillance data by the military is inherent to the role of the armed forces, including navies. In the context of discussions over its surveillance mandate, the German Navy, for example, relies on Article 87A of the Grundgesetz or Basic Law (Germany’s Constitution) which states:
(1) The Federation shall establish Armed Forces for Defense purposes. Their numerical strength and general organizational structure shall be shown in the budget.
(2) Apart from Defense, the Armed Forces may only be used insofar as explicitly permitted by this Basic Law.

290. By way of contrast Article 23 of Finland’s Territorial Surveillance Act (755/2000, as amended) specifically designates the military to be a ‘territorial surveillance authority’ alongside the frontier guard, police and customs authorities and officials assigned to territorial surveillance.

291. Article 24 goes to provide that:

The military authorities are responsible for the implementation of territorial surveillance and the cooperation of the territorial surveillance authorities.

4.1.2 What data is collected?

292. Assessing precisely what surveillance data is collected by Europe’s navies is necessarily a somewhat imprecise task. Not only is military data itself classified but detailed information about the data acquisition mechanisms is too. Finland, for example, like other European countries, has a radar monitoring system the details of which are classified. Furthermore the data provided by that system is classified as, in itself, it would betray information about the capacity of the radars.

293. Nevertheless it is possible to surmise that surveillance data is directly acquired through the use of:

(a) physical observation from vessels (including Navy and Coastguard vessels);
(b) physical observation from aircraft (which may belong to the navy or airforce);
(c) unmanned aircraft and drones;
(d) remote sensing;
(e) coastal radars; and
(f) underwater sensors to detect submarines;

294. In addition, as will be seen below, Europe’s navies also typically make use of civilian surveillance data through a range of formal and informal data sharing mechanisms. The overall objective of this data acquisition is to maintain a ‘recognised marine picture’.

4.1.3 Why is the data collected?

295. As already mentioned, surveillance data is collected for defence purposes, such notion now typically including defence against terrorist activities.

4.1.4 Who has a right to the data?

296. Once a recognised marine picture has been compiled, that combines both classified Naval data and non-classified data including data from civilian sources, it
is typically retained within the relevant Navy. The issue of sharing such data is considered in more detail below.

4.2 SIVE

4.2.1 Background

297. Ensuring control over the EU’s Southern maritime borders is a major challenge of the coastal Member States of the Mediterranean Sea and the southern Atlantic. These are the main points of entry into Europe of illegal immigrants arriving by sea from North Africa.

298. The most significant routes, which account for 70%-80% of detected illegal immigration are by small boat to Spain (particularly to the coasts of Andalucía and the Canary Islands) as well as to Italy, Malta and Greece.67

299. The Sistema Integrado de Vigilancia Exterior (SIVE) is a Spanish coastal surveillance system operated by the Guardia Civil. It was originally designed to focus on small vessels carrying illegal immigrants but is in fact used to detect, identify and intercept a range of illegal activities around Spain’s maritime frontiers. Thus current and planned uses include fisheries enforcement of closed areas, the interception of drug traffickers, the surveillance and protection of Spain’s underwater historical heritage and general surveillance of maritime traffic.

300. Nevertheless it is its small boat focus that makes SIVE somewhat unique. It is based on a range of surveillance methods including: still camera, video camera, radar and infra-red sensor. These monitors are situated on fixed stations or mobile units. The data so collected are transmitted by secure internet connection back to computers at a provincial command and control centre.

301. The first SIVE system was introduced in 2005 as a prototype in the area of the Straits of Gibraltar and comprised three mobile units, coordinated by a control centre established at the Command of the regional Guardia Civil headquarters at Algeciras.

302. Building on the success of this first phase, the SIVE has been extended to each of the six coastal provinces on the Mediterranean (from the Portuguese border through to and including Almeria) as well as the Canary Islands (Las Palmas) Gran Canarias, Lanzarote and Fuerteventura. During the course of 2008 it is anticipated that the system will extended to the provinces of Alicante, Murcia and Valencia – which face the Balearic Islands - as well as Ibiza in the Balearic Islands.

4.2.2 Legal basis

303. There is no specific legal basis for the SIVE in terms of a legal instrument that regulates its operation. Instead the overall legal basis for the SIVE is provided by

---

Ley Orgánica 2786, de Fuerzas y Cuerpos de Seguridad (Fundamental Law No. 2786 on Law Enforcement). This law regulates the actions and functions of law enforcement agencies in Spain in general and in particular the Guardia Civil

304. Spain has two separate national police forces. The Cuerpo Nacional de Policía is a civil police force while the Guardia Civil is essentially a gendarmerie. As regards border control – the Cuerpo Nacional de Policía is in charge of documentation verification at checkpoints while the Guardia Civil is in charge of security, luggage and works together with the customs service which is dependent on the ministry of finance.

305. The Guardia Civil is also responsible for policing the security of Spain’s maritime borders. Indeed the Guardia Civil is in charge ensuring order within Spain’s territorial waters including responsibility for illegal immigration, trafficking, fishing etc.

4.2.3 What data is collected?

306. The data gathered are video images, radar signals and infrared signals. The radar system is specifically set up to identify small vessels. Once a vessel is detected an operation is usually immediately launched to apprehend the vessel and its occupants.

307. The radar and infra-red images only show points on a screen that can be used to locate individual vessels. The camera images are shown on screen. As the target vessels of the SIVE are small they usually do not have identifiable numbers or names on them. It is sometimes possible to identify the faces of individuals on the boats through the camera images. The informal opinion of Guardia Civil officers consulted is that such images are not personal data as it is usually not possible to identify an individual from the image.

308. Later in 2008 it is, however, planned to integrate AIS data into the SIVE system. This data will be provided by the Ministry of Transport (Fomento) which is responsible for the operation of Spain’s AIS network.

4.2.4 Why is the data collected?

309. The data is gathered in order to detect illegal immigration as well as other illegal activities around Spain’s maritime frontiers.

4.2.5 Who has a right to the data?

310. Data collected through the SIVE is used only by the Guardia Civil which, as outlined above, normally responds directly to each incident. If, however, help is needed from another agency, such as the navy, the information gathered from SIVE such as the coordinates, approximate speed and course of a suspicious vessel are transmitted to enable an interception to take place, but not the image itself.

311. SIVE images (video, infra-red and radar tracking) are retained within the computer system if the detection/interception of suspected illegal immigrants and/or drug traffickers may result in criminal proceedings being taken
through the judicial preliminary inquiry phase. If no prosecution is envisaged, the images are retained for one month and then disposed of.

4.2.6 Data sharing in practice

312. SIVE data is not shared between individual SIVE centres because given that interception operations are local, this would not add any value. Nor is the data shared with any other agencies, simply because it is of not of interest to them.

4.3 Vessel Traffic Services (VTS)

4.3.1 Background

313. Vessel traffic services (VTS) are shore-based systems which range from the provision of simple information messages to ships, such as the position of other traffic or meteorological hazard warnings, to the extensive management of traffic within a given port or waterway. They are described by the IMO as:

   a service implemented by a Competent Authority, designed to improve the safety and efficiency of vessel traffic and to protect the environment. The service should have the capability to interact with the traffic and to respond to traffic situations developing in the VTS area.

314. There are two basic types of VTS: port VTS and coastal VTS.

315. A port VTS is primarily concerned with the management of vessel traffic to, from and within a port or harbour or harbours.

316. A coastal VTS is mainly concerned with vessel traffic passing through a specific area.

317. A VTS could also be a combination of both and indeed it is not uncommon for separate VTS to be linked. The Port of Antwerp in Belgium, for example, has its own internal VTS that is used to regulate the movement of vessels within the port. Access to and from the port, however, is regulated by the VTS of the River Scheldt, the river which links Antwerp to the sea via the Netherlands, and which is operated jointly by Belgium and the Netherlands.

318. While the River Scheldt VTS provides a traffic management service, coastal VTS often provide nothing more than an information service.

319. Usually, when a ship enters a VTS area the first duty that is imposed on the master is to report to the VTS authorities. Thereafter ships must keep watch on a specific frequency for navigational or other warnings, while they may be contacted directly by the VTS authority if there is risk of an incident or, in areas where traffic flow is regulated, to be given advice on when and how to proceed. The reason why VTS is described in this section and not in the previous section is that the activities and movements of a vessel within a VTS area are usually monitored by the VTS authority.

---

68 It would also be relatively expensive to transmit such data.
69 www.vts-scheldt.net/
Most VTS systems routinely make use of various means of surveillance data acquisition, including radar systems, as well as AIS. Some VTS also have radio direction finders (RDF) and remote video cameras. The basic purpose of monitoring vessel traffic is to ensure compliance with the relevant rules of the VTS in question.

### 4.3.2 Legal basis

In terms of international law the legal basis for VTS is currently contained in Regulation 12 of SOLAS which provides as follows:

1. Vessel traffic services (VTS) contribute to safety of life at sea, safety and efficiency of navigation and protection of the marine environment, adjacent shore areas, work sites and offshore installations from possible adverse effects of maritime traffic.

2. Contracting Governments undertake to arrange for the establishment of VTS where, in their opinion, the volume of traffic or the degree of risk justifies such services.

3. Contracting Governments planning and implementing VTS shall, wherever possible, follow the guidelines developed by the Organization. The use of VTS may only be made mandatory in sea areas within the territorial seas of a coastal State.

4. Contracting Governments shall endeavour to secure the participation in, and compliance with, the provisions of vessel traffic services by ships entitled to fly their flag.

5. Nothing in this regulation or the guidelines adopted by the Organization shall prejudice the rights and duties of Governments under international law or the legal regimes of straits used for international navigation and archipelagic sea lanes.

Further guidance on VTS is provided by Resolution A.857(20) adopted on 27 November 1997 on Guidelines for Vessel Traffic Services (the VTS Guidelines). The VTS Guidelines contain a number of references to surveillance and the acquisition of data. At paragraph 2.5.2.1, for example, the VTS Guidelines state:

A VTS should at all times be capable of generating a comprehensive overview of the traffic in its service area combined with all traffic influencing factors. The VTS should be able to compile a traffic image, which is the basis for its capability to respond to traffic situations developing in its service area. The traffic image allows the VTS operator to evaluate situations and make decisions accordingly. Data should be collected to compile the traffic image. This includes:

1. data on the fairway situation, such as meteorological and hydrological conditions and the operational status of aids to navigation;
2. data on the traffic situation, such as vessel positions, movements, identities and intentions with respect to manoeuvres, destination and routing;
3. data of vessels in accordance with the requirements of ship reporting and if necessary any additional data, required for the effective operation of the VTS.

The following paragraph goes on to note that, ‘Vessel’s reports by communication between vessels and the VTS Centre should also be used as a major source of necessary data’.

As regards the VTM Directive, VTS is addressed in a single article, Article 8, as follows:

Member States shall monitor and take all necessary and appropriate measures to ensure that:

(a) ships entering the area of applicability of a VTS operated by one or more States, of which at least one is a Member State, within their territorial sea and based on the guidelines developed by the IMO,
participate in, and comply with, the rules of that VTS;

(b) ships flying the flag of a Member State or ships bound for a port of a Member State and entering the area of applicability of such a VTS outside the territorial sea of a Member State and based on the guidelines developed by the IMO, comply with the rules of that VTS;

(c) ships flying the flag of a third State and not bound for a port in a Member State entering a VTS area outside the territorial sea of a Member State, follow the rules of that VTS wherever possible. Member States should report to the flag State concerned any apparent serious breach of those rules in such a VTS area.

325. Furthermore Article 9(3) of the VTM Directive states:

Member States shall ensure that the coastal stations in charge of monitoring the compliance with vessel traffic services and ships' routing systems have sufficient and properly qualified staff available, as well as appropriate means of communication and ship monitoring and that they operate in accordance with the relevant IMO guidelines.

4.3.3 What data is collected?

326. Apart from reporting data from participating vessels within the VTS area, the principal data collection mechanisms used by VTS are AIS and radar. Sometimes, as radar is more accurate and immediate, AIS data is laid over the radar image. This is because, as described above, a ship manoeuvring at low speed will send out fewer signals. In addition a number of VTS have high resolution video cameras that relay an image back to the VTS control centre.

4.3.4 Why is the data collected?

327. The VTS Guidelines state that the ‘purpose of vessel traffic services is to improve the safety and efficiency of navigation, safety of life at sea and the protection of the marine environment and/or the adjacent shore area, worksites and offshore installations from possible adverse effects of maritime traffic’.

4.3.5 Who has a right to the data?

328. Paragraph 2.5.4 of the VTS Guidelines is concerned with the retention of data in a database. It states:

A VTS authority should have, if necessary for the operation of the service, a database with the capacity to retain, update, supplement and retrieve data once collected. Any data retained in a system for further use should be made available only on a selective and secure basis.

4.4 CleanSeaNet

4.4.1 Background and legal basis
CleanSeaNet is a satellite-based monitoring system for marine oil spill detection and surveillance in European Waters provided by the European Maritime Safety Agency (EMSA).

The aim of CleanSeaNet is to provide oil spill detection services to the 23 Coastal States as well as to EFTA countries, Norway and Iceland.

At present CleanSeaNet is used primarily for wide area monitoring of illegal discharges from vessels at sea. It is also used on request by Member States in response to oil spill accidents and emergencies at sea. In the future it is intended that CleanSeaNet will also be able predict the drifting of accidental spills so as to facilitate the targeting of clean-up activities. The use of oil spill models for spill hind casting (back tracking) to link the detected spill with the vessel source for polluter identification is also being evaluated

CleanSeaNet uses radar images acquired by Synthetic Aperture Radar (SAR) sensors on polar orbiting satellites ENVISAT and RADARSAT 1 and 2. Such sensors provide wide area coverage (up to 400 square kilometres) and allow the detection of oil slicks on the sea surface in both darkness and daylight hours even through cloud cover. Essentially, providing the waves are of an appropriate size, the images show areas of smooth water which are caused by oil slicks.

The images are purchased by EMSA from a commercial consortium and distributed free of charge to Member States on request. Member States seek to coordinate the satellite data with their own surveillance activities using fixed wing aircraft and patrol vessels. Typically requests also seek to focus on known ‘hot spots’. A major task for EMSA is to plan the monthly acquisition of satellite data in response to the requests from the Member States.

CleanSeaNet began to operate in April 2007 following the conclusion of a tender launched in 2006 for a Europe-wide oil spill monitoring service. The tender was won by the Norwegian firm Kongsberg Satellite Services (KSAT) in Norway with consortium partners, Edisoft from Portugal, Telespazio from Italy and as well as various junior partners.


Article 1(1) of the EMSA Regulation provides for the establishment of EMSA ‘for the purpose of ensuring a high, uniform and effective level of maritime safety, maritime security …, prevention of pollution and response to pollution by ships within the Community’.
337. Article 1(3) goes on to provide that EMSA ‘shall provide Member States and the Commission with technical and scientific assistance in the field of accidental or deliberate pollution by ships and support on request with additional means in a cost-efficient way the pollution response mechanisms of Member States, without prejudice to the responsibility of coastal States to have appropriate pollution response mechanisms in place and respecting existing cooperation between Member States in this Field…’

![Fig 4. Oil spill off the northern coast of Germany (© ESA European Space Agency / EMSA 2007). This image, taken by ENVISAT-ASAR off the northern coast of Germany in the Baltic Sea on 23 June 2007, shows a distinct elongated dark feature with sharp edges and a diffused tail, typical of an oil spill being transported by the wind. This illegal oil spill was verified by the German authorities.](image)

338. The detailed tasks of EMSA are specified in Article 2 which provides *inter alia* that EMSA shall

(c) It shall work with the Member States to:

(i) organise, where appropriate, relevant training activities in fields which are the responsibility of the port State and flag State;

(ii) develop technical solutions and provide technical assistance related to the implementation of Community legislation;

(iii) support with additional means in a cost efficient way, via the Community mechanism in the field of civil protection established by Decision 2001/792/EC, Euratom, their pollution response actions in case of accidental or deliberate pollution caused by ships, when such a request has been presented. In this respect, the Agency shall assist the affected Member State under which the cleaning operations are conducted.

339. Article 10 (2)(a) of the Ship Source Pollution Directive requires EMSA to:

work with the Member States in developing technical solutions and providing technical assistance in relation to the implementation of this Directive, in actions such as tracing discharges by satellite monitoring and surveillance.

4.4.2 What data is gathered?

340. An alert report is produced for every planned image to inform the Member States of the results of the analysis, *i.e.* whether possible oil slicks are detected or
not. In case slicks are detected, the affected Coastal State immediately receives an alert to enable rapid action to be taken in order to verify and quantify the slick and to identify the potential source. The complete process, from satellite overpass to the alert, takes a maximum of 30 minutes.

341. In the future it is planned that AIS data will be displayed as an information layer over the satellite images to identify individual vessels.

342. In the future it is also intended that CleanSeaNet will be supplied with the AIS data to be acquired by and through SafeSeaNet (see section 5.3 below) via the proposed STIRES database.

4.4.3 Why is the data gathered?

343. As described the data is gathered in order to identify illegal oil discharges and accidental oil spills.

4.4.4 Who has a right to the data?

344. The Member State authorities responsible for marine pollution.
5 Data sharing mechanisms

345. A range of different mechanisms currently exist for sharing maritime surveillance data. These mechanisms serve a range of different purposes and involve a range of stakeholders. They provide for the sharing of maritime surveillance data both internationally and within individual Member States.

346. While practice as regards data sharing varies from state to state, and the aim of this report is not to catalogue all data sharing mechanisms within the EU, it is noteworthy that within some Member States Data Surveillance Sharing Mechanisms enable data to be shared among different agencies for a range of different purposes. At the international level, however, such mechanisms and planned mechanisms are all single-purpose. In other words such mechanisms enable data to be shared only among navies or navigation authorities etc.

347. With one exception they are all state funded and involve state actors.

5.1 National data sharing mechanisms

348. Practice varies within the Member States with regard to the exchange of maritime surveillance data. In some countries little sharing takes place. Elsewhere informal arrangements exist.

349. In the United Kingdom, for example, the coastguard stations of the Maritime & Coastguard Agency (MCA) receive AIS data feeds every 12 seconds. The MCA itself also receives feeds every 12 seconds but then filters the data down to every 30 seconds. This data is then made available to any party, approved by the MCA, that has a legitimate reason to require the data and that will not derive any commercial advantage from it.

350. As already mentioned, AIS data is passed freely to government departments (including DEFRA) and the Police. There is also a direct feed of the raw data to Naval Intelligence at Northwood, the Headquarters of Commander in Chief Fleet, which then mix it with their own data and distribute in accordance with their own rules for security purposes (NATO, etc).

351. A number of more formal data sharing arrangements exist.

5.1.1 France

5.1.1.1 Background and legal basis

352. SPATIONAV is an information system that is designed to collect and compile data generated by a range of sensors with a view to integrating all data available to establish surface situations to assist surveillance maritime operational centres in the performance of their duties. The principal partners in SPATIONAV are the Navy (under the Ministry of Defence), the Directorate of Maritime Affairs (DMA) (under the Ministry of Ecology, Energy, Sustainable Development and Land Planning and the Customs Department (under the Ministry of the Budget, Public Accounting and
Public Service). Their respective budget contributions are 90%, 9% and 1%. These three agencies all play an important role in maritime security.

353. The primary responsibility of the Navy is to ensure the security of French territory. It also plays an important role in the fight against pollution. The Navy administers and operates a network of coastal signal (observation) stations\(^{73}\) for coastal surveillance. In addition to the national fleet, the Navy through the Maritime Police (Gendarmerie maritime) manages a fleet of small speed boats dedicated to the policing of activities close to shore.

354. The Customs Department is responsible for enforcing customs and tax related legislation in the territorial sea and the contiguous zone and for detecting and curbing illegal trafficking throughout the waters under national jurisdiction. It administers Operational Customs Centres throughout continental France. It also participates in pollution protection and surveillance of fishing operations using so-called Polmar aircraft equipped with remote sensing technology and 16 small aircraft dedicated to maritime surveillance.

355. The DMA is responsible for maritime safety and security through its operational arm, the Regional Operational Centres for Surveillance and Rescue (CROSS)\(^{74}\). Principal missions of the CROSS are four-fold: (a) SAR; (b) maritime traffic surveillance; (c) pollution surveillance; and (d) surveillance of fishing operations. 5 CROSS have been set up in continental France, out of which three, namely CROSS Gris-Nez, CROSS Joburg and CROSS Corsen, are established in the British Channel and North Sea area and are primarily responsible for navigation control and surveillance in the traffic separation scheme in the British Channel and Pas-de Calais region. The CROSS Atlantic, located in Brittany, is, among other things, responsible for ensuring compliance with the European fisheries regulations. A large part of the operational activities of the CROSS located in the Mediterranean region is devoted to monitor navigation by pleasure crafts. The DMA manages and operates its own naval assets.

356. The objective of SPATIONAV is to strengthen land security, traffic safety, and protection of internal and territorial waters outside port areas, the EEZ, SAR areas and other specified zones. The system is regionally based with three independent systems:

- SPATIONAV English Channel/Atlantic Ocean;
- SPATIONAV Mediterranean Sea; and
- SPATIONAV West Indies/Guyana.

357. Data generated by sensors deployed along the coastline are sent to the relevant regional SPATIONAV centre. Information collected by SPATIONAV is mainly provided by coastal observation stations and AIS. The information generated by the coastal observation stations include: the name of the vessel, nature of cargo, number of persons on board, maximal draught and destination of the vessel.

---

\(^{73}\) 59 as of June 2005.

\(^{74}\) Acronym in the French language standing for Centres Régionaux Opérationnels de Surveillance et de Sauvetage.
358. SPATIONAV operates alongside another mechanism that has data-sharing features, namely, TRAFIC 2000. TRAFIC 2000, which was developed to implement the VTM Directive, is the French system for monitoring maritime merchant traffic within waters under national jurisdiction.

359. The primary goal of TRAFIC 2000 is to provide information enabling the authorities responsible for maritime security to assess the risks or threats on security, safety and the environment by any vessels, including defective vessels and vessels carrying dangerous or polluting goods, and take preventive actions where necessary. In addition, this system facilitates the intervention of maritime authorities in cases of emergency, the control of vessels by port authorities and the management of port facilities. While TRAFIC 2000 is operated by a special information unit located in the CROSS Joburg in Cherbourg\(^\text{75}\) with the technical support of the Maritime Information System Department under the DMA, HAZMAT-related information is provided by the CROSS and port authorities.

360. To date, all French autonomous ports, except the Port of Marseille\(^\text{76}\), are connected to TRAFIC 2000 and provide information on vessels’ arrival at, and departure from, ports and on the nature of the dangerous or polluting goods on board. The DMA has entered into discussion with the Port Directorate to make arrangements with ports other than autonomous ports with a view to collecting quality information from all ports in France\(^\text{77}\). The CROSS provide information on vessels’ movements. Information transmitted by port authorities and CROSS are automatically incorporated in the database and can be consulted by the competent authorities through the intranet network. By virtue of Article 9(2) of the VTM Directive, the system is intended to be integrated in the SafeSeaNet\(^\text{78}\) so as to allow the monitoring of maritime traffic throughout European territorial waters, prevent accidents at sea and, by extension, marine pollution. While connection of TRAFIC 2000 to SafeSeaNet is technically feasible, the French Government has so far refrained from doing so on the basis that confidentiality requirements under SafeSeaNet are not adequate as they do not provide sufficient protection for commercially valuable information. Confidentiality requirements are currently being reviewed and France expects to connect TRAFIC 2000 to the European system by the end of 2008 as required by the VTM Directive.

361. The main information contained in TRAFIC 2000 includes –

Static information concerning vessels:
(a) Vessel’s identification;
(b) Vessel’s name;
(c) Nationality of the vessel;

Voyage information:

\(^{75}\) This information unit is under the supervision of the Bureau of Rescue and Maritime Traffic (SM1) placed under the control and responsibility of the Maritime Security Department under the Direction of Maritime Affairs.

\(^{76}\) The port of Marseille is expected to be connected to TRAFIC 2000 by summer 2008.

\(^{77}\) By virtue of the Decentralization Law of 2004 as modified in 2007, most important commercial ports remain under the responsibility of the State and have the legal status of autonomous ports. Other ports are under the responsibility of local or territorial authorities: principally regions or departments for commercial ports; departments for fishing ports; and municipalities for marinas.

\(^{78}\) See below.
(d) Port of origin;
(e) Port of destination;
(f) Intended route;
(g) Draught of the vessel;
(h) Types of hazardous goods on board in accordance with internationally accepted standards;
(i) Number of crew;
(j) Estimated time of arrival at the port of destination;
(k) Estimated time of departure from port.

362. In addition to port authorities and CROSS, information available on TRAFIC 2000 can be accessed by the Customs Department, the Navy and Maritime Prefectures. Conditions of access, disclosure and use of information contained in TRAFIC 2000 are governed by specific Conventions signed by the Director of Maritime Affairs\(^79\) and the Chief of Staff of the Navy, the Maritime Prefects and Port Directors respectively\(^80\).

363. To date, SPATIONAV V0 has been tested in the Mediterranean Sea. It is expected that SPATIONAV V1, which is an upgraded version of SPATIONAV V0, will be operational within the next 10 months according to the following time table:

(a) in the English Channel and the Atlantic Ocean by summer 2008;
(b) in the Mediterranean Sea by October/November 2008; and
(c) in the West Indies and Guyana by early 2009.

364. The principal innovation of SPATIONAV V1 will be to integrate AIS information provided by shore-based stations and AIS units on board merchant vessels and surveillance aircrafts.

365. In the medium term (horizon 2010/2012), SPATIONAV V2 should enable the integration of information from new sensors, particularly, radars HF. Preparation of SPATIONAV V3 (post 2010/2012) is under way and aimed at broadening the monitored area through the use of information from other sensors (satellite, LRIT, drones).

5.1.1.2 **What data is shared?**

366. The information received from the coastal observation stations (the name of the vessel, nature of cargo, number of persons on board, maximal draught and destination of the vessel etc.) is combined by SPATIONAV to produce a so-called “local situation”. This information is sent to the central system, based in the maritime operation centres in the maritime prefectures of Brest, Toulon and Fort de France. The central system receives information on various local situations and also data from monitoring centres fitted with AIS established throughout the coastal zone.

\(^{79}\) Head of DMA.

\(^{80}\) These Conventions were not made available to the mission for review. The term *convention*, which is the terminology used in French law, should be construed as memorandum of understanding in this context.
367. Information is visualized on a mapping system (ECDIS) where information on each represented object is shown in the form of tracks and zones and updated every 60 seconds (real time). Each such object is linked to a file containing data on, *inter alia*, identity, position, and intended route of the vessel concerned.

368. In addition, SPATIONAV will soon integrate information from TRAFIC 2000 as these two systems will be connected and information generated by each of them will be exchanged automatically. Trials to ensure compatibility of information exchange between the two systems are under way.

369. It is planned that these systems will be connected by summer 2008. SPATIONAV merges all collected information so as to create a global situation in the regional area concerned, known as the Maritime Approaches Situation (SAM\(^{81}\)) (situational awareness). The SAM is an operational tool designed to assist State administrations and agencies involved in SAS in assessing risks. Beneficiaries of the system are the Customs Department through the customs operational centres, the Directorate of Maritime Affairs through the CROSS, the Navy and the Maritime Prefect through the maritime operation centres.

5.1.1.3 *Who has a right to the data?*

370. SPATIONAV is administered by the Navy and the General Directorate of Armament placed under the Ministry of Defence. Since the SPATIONAV programme is a joint military, customs and maritime affairs effort, all information is available to every partner with no information restricted to military use only.

5.1.2 *Finland*

5.1.2.1 *Background and legal basis*

371. Finland has a well developed national maritime data exchange mechanism in place. The principal actors are the Navy (under the Ministry of Defence), the Frontier Guard (which is under the Ministry of the Interior) and the Maritime Administration (which is under the Ministry of Traffic and Communications).

372. Following a the adoption by the State Council in 1993 of a decision that noted that ‘co-operation between officials concerning maritime surveillance in Finland has to be rationalized’ the legal structure of the mechanism is provided by the 1993 Maritime Environmental Tri-Authority Operations (METO) Memorandum which was concluded between the principal actors. The memorandum also notes that other secondary actors are to be involved in the mechanism such as the police, customs, rescue etc. The memorandum built on a long tradition of inter-ministerial cooperation in the sphere of maritime surveillance.

373. Each of the principal actors has substantial maritime surveillance gathering systems in place. Finland has an extensive system of shore based AIS stations in place, operated by the Maritime Administration, in addition to wide ranging VTS

\(^{81}\) SAM is the acronym in the French language standing for “situation d’approches maritimes”.

71
radar coverage (Helsinki VTS has 32 radar stations, the Archipelago VTS has 28 radar stations, the West Coast VTS has 6 radar stations, while the Bothnia VTS has 9 radar stations). In addition the Maritime Administration has access to data from the GOFRREP reporting system while AIS data is shared with other Baltic states through Helcom.

374. The Navy has its own network of radars and sensors (around nine radars), details of which are classified, while the Border Guards obtain surveillance data from their own fixed sensors (some eight radars) as well as patrols undertaken by fixed wing aircraft and helicopters and its own patrol vessels.

375. Data from the three principal actors is sent electronically to the Naval Headquarters at Turku where it is compiled to create a real time maritime picture. The Navy then distributes the data to the other agencies in accordance with their specific needs.

5.1.2.2 What data is shared?

376. Because the Navy’s compiled maritime picture contains classified information (such as the location of its radars and other surveillance sources such as submarine sensors) it is not shared in its entirety. Nevertheless a wide range of non-classified data can be provided through the Finnish system (see Box A).

Box A – Data available in the Finnish maritime data exchange mechanism

AIS Dest Port, AIS Dimensions, AIS Draught, AIS DTE, AIS ETA, AIS Fixing Device, AIS Navstatus, AIS Time, AIS Type of ship and cargo type, Altitude-SL, Altitude-WGS84, Course Heading, Measurement Time, Number of sources, Position, ROT, Speed, Owner, Comment, Dimensions, Draught, IMO Number, International Callsign, MMSI, Name, Nationality, Ship DB, Id, Work Name, Credibility, Ident Means, Ident Timestamp, Identifier ID, Classification, Bearing frequency, Bearing signal strength, Bearing bandwidth, Bearing channel, Affiliation, Category, Exercise Affiliation, Platform, Platform activity, Platform Specific Type, Activity, Anchor Zone, Attention, Emergency GOFRREP Status, Hazard, Navigational Status, Pilot On Board, Sensor Type Strongest, Sensor Types, Tracking Quality, Tracking Status, Visit ID, XTE Enable, System ID, Security Class, Sensor ID, Sensor TNO, Track Init Time, Track Type, User ID, User ID assigner, Covariance, Cargo, ETA, ETD, ISPS, Permit, Persons, Port of Destination, Port of Origin, Route, Voyage Timestamp, Plot Sensor ID, Plot Measured Position, Plot Strength, Plot Altitude-WGS84, Plot Measurement Time, Bearing init time, Bearing measurement time, Bearing origin position, Bearing direction, Bearing information, and Bearing means.

377. The principal sources of these data are AIS, the Finnish VTS, the GOFRREP reporting system and radar and other surveillance equipment operated by the Navy, Maritime Administration and Border Guard.

5.1.2.3 Who has a right to the data?

378. In addition to the three primary actors the secondary actors are also supplied with surveillance data by the Navy. These include the environmental ministry, customs, the police and the rescue service.

---

82 A further VTS, Saimaa, covers the deepwater routes of Lake Saimaa but is reliant on AIS data.
379. Care however is taken not to provide personal data, which are defined to include names of individuals, to agencies other than law enforcement authorities such as the border guards. Such data is not, for example, provided to the Navy. For example the Border Guards receive a VMS feed directly from the Ministry of Agriculture and Forestry which is responsible for fisheries as well as the name of the crews on fishing vessels each time they put out to sea. The Navy, in contrast receives VMS data which only shows the name of each fishing vessel and the fact that it is a Finnish vessel.

5.2 Regional AIS data sharing agreements

380. A number of regional AIS sharing mechanisms have been established within Europe to date, the most formal of which is the HELCOM AIS Network.

5.2.1 HELCOM AIS Network

381. The establishment of the HELCOM AIS Network was one of the outcomes of the Declaration on the Safety of Navigation and Emergency Capacity in the Baltic Sea Area (‘HELCOM Copenhagen Declaration’) which was adopted on 10 September 2001 in Copenhagen by the HELCOM Extraordinary Ministerial Meeting.

382. HELCOM, more formally known as the Helsinki Commission, is the governing body of the 1992 ‘Convention on the Protection of the Marine Environment of the Baltic Sea Area’ more usually known as the Helsinki Convention. The present Contracting Parties to HELCOM are Denmark, Estonia, European Community, Finland, Germany, Latvia, Lithuania, Poland, Russia and Sweden.

383. By Article IV of the HELCOM Copenhagen Declaration the Contracting Parties agreed to enhance the use of AIS:

- by requiring the Governments of the Contracting Parties to establish national, landbased monitoring systems for ships, based on AIS signals. A full monitoring of the Baltic Sea Area within A1 sea area shall take place not later than 1 July 2005;
- by requiring the Governments of the Contracting Parties to establish a common Baltic Sea monitoring system based on - and with access to - all national Baltic AIS monitoring systems;
- by requiring the Governments of the Contracting Parties to provide the HELCOM Secretariat with specified and conformed AIS data in order to enable the Secretariat to prepare an annual report containing reliable statistics on ships’ traffic in the Baltic Sea Area as a basis for risk analyses and further consideration by the Contracting Parties;
- by establishing an expert working group, under the leadership of Sweden, with representatives from each of the Contracting Parties with the purpose of facilitating mutual exchange and deliveries of AIS data, including the construction of the monitoring system for the maritime traffic in the Baltic Sea Area …

384. The installation of the Baltic AIS Network was completed in 2005 with the connection of AIS coastal stations in the Contracting Parties to a central HELCOM server which is located in Copenhagen. The network enables AIS data to be sent to the HELCOM server for analysis. It also enables the sharing of such data between the Contracting Parties and Norway.

385. An agreement on Sharing AIS Information was developed by the Working Group and signed by the Contracting Parties and Norway in Spring 2005.
5.2.2 Other regional AIS Networks

386. The North Sea Data Exchange is operated by the North Sea Information Centre, a regional centre for collecting and distributing national AIS data from the national AIS networks of Norway, Sweden, Denmark, the Netherlands, Belgium and the UK. The North Sea Information Centre was established through the ‘Safety at Sea Project’ which lasted between September 2004 and June 2007 and which was funded by the European Commission under the auspices of INTERREG III.

387. AIS data from each country is freely available to the others via a central server which is also located in Copenhagen. There is no public access to this data, however.

388. It is understood that a regional AIS Network for the Mediterranean will shortly be established.

5.3 SafeSeaNet

5.3.1 Background and legal basis

389. SafeSeaNet is a system of the European Commission, operated by EMSA but not fully implemented and undergoing continuous improvement. It supports the implementation of most of Title II and parts of Titles I, III and IV of the VTM Directive.

390. In outline, it is a specialised network established to facilitate the exchange of data in an electronic format between the maritime administrations of the coastal Members States and Norway (the ‘participating countries’). The system has been developed with the objective of enabling compliance with the VTM Directive and additionally with other instruments related to port reception facilities and on port state control.

391. The implementation of SafeSeaNet began in 2002 with the objective of enabling the inter-linking of national systems in respect of four basic messages required in connection with the VTM Directive (port, HAZMAT, ship and alert notifications) by the end of 2008.

392. SafeSeaNet is not specifically mentioned in the VTM Directive, although the directive requires the Member States to be able to exchange data electronically. Specifically Article 14, which is entitled ‘Computerised exchange of data between Member States’, provides:

> Member States shall cooperate to ensure the interconnection and interoperability of the national systems used to manage the information indicated in Annex I.

Communication systems set up pursuant to the first subparagraph must display the following features:
(a) data exchange must be electronic and enable messages notified in accordance with Article 13 to be received and processed;
(b) the system must allow information to be transmitted 24 hours a day;
(c) each Member State must be able, upon request, to send information on the ship and the dangerous or polluting goods on board without delay to the competent authority of another Member State.
The reference to Annex I means that the data that is to be exchanged electronically is: (a) the data reported to ports required to be exchanged pursuant to Article 4; (b) the mainly hazmat cargo data required to be reported pursuant to Articles 12 and 13; and (c) the data reported to coastal mandatory reporting systems pursuant to Article 5.

Additionally, Article 16 requires an exchange of “alert” information on “ships posing a potential hazard to shipping or...” between a more limited range of message originators and recipients.

Furthermore, Article 23(b) requires the Member States and the Commission to cooperate in attaining a number of objectives including the development and enhancement of ‘telematic links between the coastal stations of the Member States with a view to obtaining a clearer picture of traffic, improving the monitoring of ships in transit and harmonising and, as far as possible, streamlining the reports required from ships en route’.

Therefore although Article 14 provides a relatively clear legal basis for the exchange of reporting data and hazmat data, the legal basis for the exchange of AIS data is less clear, particularly given the limited obligations of the Member States under SOLAS. Article 9(2) is cited as providing a legal basis for the exchange of AIS data. It states:

The process of building up all necessary equipment and shore-based installations for implementing this Directive shall be completed by the end of 2007. Member States shall ensure that the appropriate equipment for relaying the information to, and exchanging it between, the national systems of Member States shall be operational at the latest one year thereafter.

Article 9(1) in fact refers explicitly to coastal AIS stations: it imposes a duty on the Member States to provide these in a timetable compatible with the duty imposed on vessel owners to install AIS. The fact is, though, that Article 9(2) does not specifically refer to AIS.

EMSA decided to develop in 2008/2009 a new SafeSeaNet module (named STIRES – SafeSeaNet Traffic Information Relay and Exchange System) in order to create a tracking system based at least initially, on AIS information provided by the national and regional AIS networks of the Member States. Combined with full standard Electronic Navigational Charts, this will provide Geographic Information System (GIS) platform for other related applications and services consist with the aims of the directive.

In the future it is also envisaged (subject to the necessary security safeguards) that SafeSeaNet will be used to distribute LRIT data although as described above, provisions on LRIT are not yet contained in the VTM Directive.

SafeSeaNet, which is still in its Version 1, is not yet entirely implemented by all Member States. Essentially an index server which provides indication as to where the relevant reporting and hazmat data is held and can be obtained electronically, SafeSeaNet must still undergo a number of improvements, currently hindered (except for STIRES) from full progress by delays in the legal, planning

and decision making process. It also contains very little real time data to show where the ships are actually situated. But with STIRES, it will be fed with real time data from existing regional AIS Networks in the Baltic, North and Mediterranean Seas. Indeed, it was not originally designed to provide a real time picture. It is anticipated that with STIRES, the system will be able to provide a near-real-time picture of shipping throughout most of the EU. Meeting the full official implementation date (end of 2008) and STIRES are viewed as the principal objectives at this time.

401. The most recent SafeSeaNet Quarterly Report for the first quarter of 2008 (the Implementation Report) shows that implementation so far, continues to be slow (see Table 1 below).

<table>
<thead>
<tr>
<th>Country</th>
<th>Notifications</th>
<th>Date Projected for Tests or Production</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Port</td>
<td>Hazmat</td>
</tr>
<tr>
<td>BE Belgium</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>BU Bulgaria</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>CY Cyprus</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>DK Denmark</td>
<td>ready</td>
<td>yes</td>
</tr>
<tr>
<td>EE Estonia</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>FI Finland</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>FR France</td>
<td>ready</td>
<td>ready</td>
</tr>
<tr>
<td>DE Germany</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>GR Greece</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>IC Iceland</td>
<td>ready</td>
<td>ready</td>
</tr>
<tr>
<td>IE Ireland</td>
<td>ready</td>
<td>ready</td>
</tr>
<tr>
<td>IT Italy</td>
<td>yes</td>
<td>ready</td>
</tr>
<tr>
<td>LV Latvia</td>
<td>ready</td>
<td>ready</td>
</tr>
<tr>
<td>LT Lithuania</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>MT Malta</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>NL Netherlands</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>NO Norway</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>PL Poland</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>PT Portugal</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>RO Romania ('*')</td>
<td>yes ('*')</td>
<td>yes ('*')</td>
</tr>
<tr>
<td>SI Slovenia ('*')</td>
<td>yes ('*')</td>
<td>yes ('*')</td>
</tr>
<tr>
<td>ES Spain</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SE Sweden</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>GB United Kingdom</td>
<td>ready</td>
<td>ready</td>
</tr>
</tbody>
</table>

Notes: Update: 02 April 2008
(* ) Countries participating using the Web interface.
(**) Delayed due to problem with the digital certificate
Yes Participating, sending notifications
Ready
Passing the "commissioning" tests that certify national compliance with SSN but not yet using the system
No No connection to SSN

Table 1. SafeSeaNet implementation

402. Another table in the Implementation Report sets out the numbers of notifications and requests made in the first quarter of the year (see Table 2). EMSA’s observations on these figures are that ‘although most of the countries have proved their technical capability for developing their (SafeSeaNet) applications, the statistics indicate that they must extend their efforts beyond technical implementation into routine operations. Though increasing, the number of the notifications falls short of what is expected for the system in production for all messages’.
Table 2. SafeSeaNet notifications and requests

403. Of the notifications nearly 95% are from AIS with mandatory reporting system notifications being provided only by Italy and Slovenia, notwithstanding the existence a number of reporting systems within the waters of the participating countries such as WETREP, CALDOVEREP, GOFREP.

404. Another important finding of the Implementation Report was that the ‘quality of data annexed to the messages is still poor and consequently, the data exchanged through SafeSeaNet is not fully reliable’. The most relevant examples are cited as follows:

- About 30% of the messages are found incorrect or incomplete, mainly because the source of the information was incorrect or incomplete;
- Port and HAZMAT messages omit the “total number of persons on board” as required by the Annex I of the Directive in 52% of the messages exchanged;
- Further improvements should be made to the Ship Notifications messages, as the port of destination is not provided in 41% of the messages exchanged;
- A comparison with external sources indicates that not all the port authorities in the SafeSeaNet participating countries are notifying SafeSeaNet with Port Notifications as required by Article 4 of the Directive.

5.3.2 What data is shared?

405. SafeSeaNet is currently essentially an index server which provides indication as to where the relevant reporting and hazmat data is held and can be obtained electronically. It is still in an intermediate stage.

406. It contains very little real time data other than a live feed from the Helcom AIS Network. SafeSeaNet must still undergo a number of improvements, currently hindered (except for STIRES) from full progress by delays in the planning and decision making process. It also contains very little real time data. With STIRES, it will be fed with real time data from existing regional AIS Networks in the Baltic, North and Mediterranean Seas.

407. The actual data is held at the Member State level, but it is indexed, and that indexed information is stored and is accessible to Member States via the European
Index Server (EIS). The distributed architecture of SafeSeaNet is made up of three levels: (i) the Local Competent Authorities (LCA); the National Competent Authorities; and the EIS.

5.3.3 Who has a right to the data?

408. The LCA are the data providers and end users including port authorities and coastal stations. LCA are both the recipients and suppliers of SafeSeaNet messages, subject to their right of access. The LCA of the national authority (e.g. MRCCs, port state control) are considered to be the main requesters of information from the system.

409. Essentially any SafeSeaNet data request is directed to the EIS, which then forwards the request based on the index to the relevant Member State. The relevant Member State would retrieve and send, via the EIS, the required data to the requesting Member State. Therefore, the SafeSeaNet system does not provide a ‘real time’ picture of ship traffic activity. Further, access to the SafeSeaNet system is restricted: access to the EIS in Member States is centralised, and individual users must be registered with the National Competent Authority before access can be gained to SafeSeaNet data.

410. One of the concerns that have been raised about SafeSeaNet relates to the seeming lack of a formal and robust data policy particularly as regards the Hazmat data (as described in the case of France, above). This data is considered by ports and port authorities to be highly commercially confidential as it could provide a relatively complete picture of the movement of a range of different types of cargo e.g. bulk oil.

411. Ports in particular are concerned that such information if used inappropriately, might cause them commercial harm if passed on to a rival. For this reason a number of ports through their Member States will only reveal their data in a non-processable ‘pdf’ format. More specifically, the actual circumstances in which detailed data can be requested are not clearly specified. Furthermore, while data can only be requested by recognised SafeSeaNet participants, it is up to the National Competent Authority of each Member State to ensure that the data does not end up in ‘the wrong hands’. Expected amendments to the VTM Directive may provide an opportunity to address this as well as a number of other concerns.

5.4 Commercial AIS data sharing mechanisms

5.4.1 Background and legal basis

412. As already described, because AIS data is unencrypted and broadcast over publicly available wavelengths there is nothing to stop third parties, apart than other vessels and the authorities of Coastal States, from gathering it. Some of this information is gathered by hobbyists or by port authorities. However, the commercial value of AIS data is such that a number of companies have successfully established commercial web-based AIS data sharing mechanisms.

---

84 The EIS is hosted on a platform of the Commission’s Informatics Directorate.
413. The first commercial service, and one of the largest, is ‘AISLive’ which is provided by AISLive Limited, a UK subsidiary of LRF (which as described in section 2.2 above is the sole authority for issuing IMO ship identity numbers).85

414. The AISLive network, which began operation in 2004 and currently has more than 107,000 users, provides real-time information from over 2,000 locations around the world and shows the live positions of 26,000 vessels a day through a web-based service. The services are exclusively available to commercially vetted companies engaged in the maritime industry.86

415. The effect of such services is that a far broader range of maritime actors can have access to AIS data including port authorities, customs authorities and pilots. They can also contribute to the identification of oily ballast discharges and a new role is seen in tracking the emission by commercial vessel of exhaust pollutants (principally SOx and NOx). AISLive for example provides AIS data to a wide range of official agencies around Europe as well as the European Commission and EMSA.

416. AISLive obtains AIS feeds from a range of sources including a North American maritime shipping information exchange, ships and shipping companies as well as a range of privately operated receivers that are either sold to the operators by AISLive or given away. The basic deal is that anyone supplying data to AISLive is entitled to a free subscription to the AISLive website.

417. The installation of an AIS receiver is a simple matter. The receiver is attached to a digital box from which the data is sent via the internet to the central server of the service in question.

418. Prior to starting operations AISLive Limited held extensive consultations with Office of Communications (Ofcom) the independent regulator and competition authority for the UK communications industries as to whether or not it was necessary to obtain a licence for each AIS receiver. As the receivers operate on VHF frequencies and are ‘receive only’ Ofcom concluded that they did not. Given that the Federal authorities in the United States had apparently taken the same view, the view was taken that in principle such licences should not be necessary elsewhere.

419. Finally, the possible development of another business model for the commercial acquisition and supply of AIS data should be mentioned. In June 2004 the US satellite telecommunications company ORBCOMM Inc, was awarded a contract by the United States Coast Guard to develop and supply AIS acquisition capability via its satellite network. Space based AIS is not expected to be a live data source until 2010 as the first test was launched in Summer 2008 and given the substantial start up costs is likely to be substantially more expensive for subscribers than the existing commercial services.

86 Previously a free limited coverage, time delayed website attracted some 125,000 users. The free service has now been discontinued in order to vet potential subscribers.
5.4.2 What data is shared?

420. The data that is supplied through the commercial networks is the basic AIS data namely vessel position, IMO number, MMSID, latitude, longitude, course, speed and next port of call. The limited and optional cargo information that may be transmitted under AIS is not provided by AIS Live, not least because it is not considered reliable. The basic AIS data can then be layered onto a digital chart to give a graphical representation of vessel location (and course). A range of different services are available from each commercial provider relating to the format or scope of the data varying from a raw live feed to a supply which has been ‘cleaned’ through database analysis, client specific extracts and analysis of historic movements. The data is delivered via the internet.

5.4.3 Who has a right to the data

421. Although AISLive offers free trials of its services these are only supplied to those who register and who appear to have a valid reason for doing so (because they are involved in the merchant shipping sector for example). Trial registrations have been refused for those who do not meet this standard. The trial service is the same service open to a fully paid for subscription and vessel positions are updated every three minutes.

422. Thereafter the right to data depends on the particular package that is purchased from the commercial supplier.

5.4.4 Are there any restrictions on further sharing the data?

423. As these are commercial services the contractual licence agreements place restrictions on the use and re-use/sharing of the data.

5.5 Finland/Sweden

5.5.1 Background and legal basis

424. Since 2006 the Finnish and Swedish navies have routinely exchanged their respective compiled maritime pictures. This arrangement which is known as SUCFIS is undertaken on the basis of a memorandum of understanding dated 2005 between the Finnish Ministry of Defence and the Swedish Armed Forces. The reporting and surveillance systems of the two countries are completely separate but are linked through a technical bridge.

425. In accordance with the memorandum of understanding, both parties have agreed to provide all information necessary to establish a compiled marine picture but equally both parties have retained the right to limit any information given without any need to provide a reason for this. However they have agreed to indicate to the other if any information is withheld.

5.5.2 What data is shared?
426. Because the information relates to the classified compiled maritime picture it is not possible to describe precisely what data is exchanged, save to say that it concerns all surface vessel activity in the Southern Baltic.

5.5.3 Who has a right to the data and are there any restrictions on data sharing?

427. Once the data has been exchanged it is safeguarded in accordance with relevant national legislation. There are safeguards but these are technical. Information received can be supplied to other state agencies but only for official purposes. Thus data received from Sweden pursuant to SUCFIS can be forwarded to the Finnish Border Guards, Maritime Administration or the police, customs or fisheries administration. Such data cannot, however, be released to any third country or to any non-official user without specific approval from Sweden.

5.6 MAOC-N

5.6.1 Background and legal basis

428. The Maritime Analysis and Operations Centre – Narcotics (MAOC-N), which is based in Lisbon, Portugal, is a law enforcement coordination centre that uses maritime surveillance data in order to plan and coordinate the execution of maritime interdiction operations and provides such data as may be necessary to those naval and other forces that physically undertake interdictions.

MAOC-N was established 30 September 2007 on the basis of an agreement concluded between Ireland, the Netherlands, Spain, Italy, Portugal, France and the United Kingdom (the MAOC-N Agreement). By Article 2(2) of the MAOC-N Agreement the Parties, agreed that acting through MAOC-N, they will:

a) Collect and analyse information to assist in determining best operational outcomes in relation to illicit drug trafficking by sea and by air in the operational area.

b) Enhance intelligence through information exchange among themselves and, in the appropriate manner, with Europol.

c) Endeavour to ascertain the availability of their assets which, where possible, shall be notified in advance, in order to facilitate interdiction operations to suppress illicit drug trafficking by sea and by air.

429. In outline the main task of MAOC-N is to coordinate the interdiction on the high seas of vessels trafficking illegal drugs. Such interdictions take place in accordance with the provisions of Article 17 of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances which was concluded on 20 December 1988 in Vienna (the Vienna Convention). Such interdictions may take place at the request of the flag State or with the permission of the latter.

430. Article 17(2) provides that a State which has ‘reasonable grounds to suspect that a vessel flying its flag or not displaying a flag or marks of registry is engaged in illicit traffic may request the assistance of other Parties in suppressing its use for that purpose’. Parties receiving such a request must ‘render such assistance within the means available to them’.
Article 17 (3) provides that:

A Party which has reasonable grounds to suspect that a vessel exercising freedom of navigation in accordance with international law, and flying the flag or displaying marks of registry of another Party is engaged in illicit traffic may so notify the flag State, request confirmation of registry and, if confirmed, request authorization from the flag State to take appropriate measures in regard to that vessel.

If the flag State of a vessel is not a party to the Vienna Convention then a boarding may take place on the basis of a bilateral agreement with the flag State pursuant to Article 108 of the LOSC which is a similar provision to Article 17(2). It states:

Any State which has reasonable grounds for believing that a ship flying its flag is engaged in illicit traffic in narcotic drugs or psychotropic substances may request the cooperation of other States to suppress such Traffic.

5.6.2 What data is gathered?

In order to discharge its functions MAOC-N deals with a broad range of information ranging from open source data to classified intelligence. Consequently data security is a major issue. MAOC-N has access to AIS data (either from the navies or other administrations of the participating states) or through commercial AIS data providers. At present VMS data is not acquired although this is seen as being desirable. It is currently perceived that the future acquisition of LRIT data will be more difficult.

Surveillance data acquired by MAOC-N is retained within the centre. It is also actionable in that each participating country declassifies any material provided so that it can be structured into an operational plan for interdiction. Each Country Liaison Officer is responsible for acting within the existing protocols and gateways, pertinent to their nation, for sharing this product.

If it is necessary for personal data to be shared in connection with an operation, for example data that persons present on a ship have criminal convictions for crimes of violence or are known to carry weapons, such data is transmitted directly by the intelligence holder to the police force of the country that will undertake the interdiction so that such data can be forwarded to the responsible authorities (such as the navy).

MAOC-N intends in due course to seek to obtain VMS data showing the position of fishing vessels. Any data received, though, would remain in a secure environment within the centre.

5.6.3 Who has a right to the data?

Article 6 of the MAOC-N Agreement, which is entitled ‘Protection of Personal Data and Other Information Provided by the Parties’, states:

1. The processing and protection of personal data and other information provided by the Parties shall be carried out in accordance with national laws of the Parties, EU law and international law binding on the Parties, including the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981.
2. Personal data and other information provided by the Parties shall not be transmitted to third States or any other entity without the prior consent of the provider of the information and may not be used for purposes other than those for which they were initially transmitted.

439. Article 12 of the MAOC-N Agreement requires MAOC-N’s Executive Board, on which a senior representative from each Party is represented and which is also responsible for appointing MAOC-N’s Director, to adopt a Procedure Handbook which must inter alia contain ‘protocols for information exchange and processing, including its protection’. This document has yet, however, to be adopted.87

5.7 V-RMTC

5.7.1 Background and legal basis

440. The Virtual Maritime Traffic Centre (V-RMTC) is a virtual network connecting the operational centres of a number of participating navies based in, and around, the Mediterranean Sea and which began formal operations in September 2006. V-RMTC is run by the Maritime Policy Office of the Italian Navy’s General Staff Third General Planning Department.

441. The legal framework for the V-RMTC, is contained in an ‘Operational Arrangement’ which was signed on 12 October 2006 on behalf of Portugal, Spain, France, Slovenia, Croatia, Montenegro, Albania, Greece, Turkey, Cyprus, Malta, Jordan, Israel, Romania, United Kingdom and the USA.88

442. The V-RMTC network enables the exchange via the internet of unclassified information on merchant shipping consisting of 300 tons or more units.

443. The Community of the 17 Signatory Countries to the Operational Arrangement is known as the “Wider Community”, in order to distinguish it from the community adhering to the “Parent Fusion Centres”. These are exactly the same as the V-RMTC, but consisting of these Countries that, for various reasons, do not wish to participate in the Wider Community.

444. There is no data exchange between the Wider Community and the Parent Fusion Centres.

445. Subsequently an additional Operational Arrangement was concluded in 30 May 2007 to establish a V-RMTC 5+5 Network that involves the Navies of Italy, France, Spain, Portugal and those of Malta, Mauretania, Morocco. This provides for a similar kind of data sharing arrangement.

5.7.2 What data is shared?

446. Section 1 of the Operating Agreement provides that each participating State ‘will supply the information in accordance with its capabilities, its laws and regulations and in accordance with maintaining the security of its state and of its

---

87 It is understood that the handbook will be adopted by mid July 2008.
88 The Federal Republic of Germany subsequently became party to the Operational Agreement.
assets’. It goes on to specify that ‘no classified information will be exchanged in the framework of the V-RMTC’.

447. Section 3 specifies that the ‘data of interest to be exchanged may consist of information about arrival and departure from national ports of the Participants, as well as the position at sea of all merchant units, excluding, at least in the initial phase, military sealift units, ferry-boats, cargo units with less than 300 tons tonnage and fishing vessels with any tonnage’. It goes on to state that the scope of the system may be broadened to include smaller vessels if this is agreed by the V-RMTC Steering Group which is foreseen by the Section 1 of the Operating Agreement.\(^\text{89}\)

448. Further information about the data to be exchanged is set out in Section 5 of the agreement. This section requires reports to be made available by each the operational headquarters of each participating Navy. The section further specifies that:

The following information will be available as a minimum:

- Ship’s name;
- International Call Sign;
- Flag;
- IMO number;
- Arrivals: port of arrival and arrival’s date in ZULU time - port of origin with departure’s date in ZULU time; or
- Departures: port of origin with departure’s date in ZULU time - port of destination with the estimated ZULU time and date of arrival; or
- Position: in Latitude and Longitude (if underway or at anchor).

449. Furthermore, data exchanges are to take place in near real time.

5.7.3 **Who has a right to the data?**

450. The scope and purpose of the data exchange are addressed in Section 7. This provides that all of the data exchanged within the V-RMTC will be available to all participating Navies. However each participating Navy is required to use the data for ‘National Defence purposes only , under their own exclusive responsibility, taking into account that access to and handling of information contained in the V-RMTC data base will be confined to the designated Operational Headquarters of the Participants which will actively contribute to the data base’.

451. The next paragraphs state:

Information contained in the V-RMTC data base will not be released to a third Country or Organisation, unless authorized by the entire V-RMTC community.

Each designated Operational Headquarters will strictly comply with the security policy and specifications attached as an Annex to this Operational Arrangement.

452. It has not been possible to obtain a copy of the Annex referred to here.

453. Similar provisions are contained in the V-RMTC 5+5 Operational Arrangement.

\(^{89}\) Each participating State is to be represented in this body which is chaired by Italy.
5.8 NATO – Marine Situational Awareness Concept

5.8.1 Background

454. The concept of Maritime Situational Awareness (MSA) is designed to confer informational superiority upon the North Atlantic Treaty Organisation (NATO) and thus to improve maritime security. A formal definition of MSA was adopted by NATO’s Military Committee on 14 January 2008 as follows:

NATO MSA is an enabling capability which seeks to deliver the required Information Superiority in the maritime environment in order to achieve a common understanding of the maritime situation in order to increase effectiveness in the planning and conduct of operations.

455. Central to the MSA concept is NATO’s Maritime Safety and Security Information System (MSSIS) which is based around the acquisition and analysis of AIS data. The MSSIS consists of two components: (a) the Transview (or TV32) software programme which is used locally to display data from an AIS receiver and upload that data to the MSSIS servers (and which can also be used to request and display data from the MSSIS servers); and (b) the MSSIS servers which collect, validate, and distribute AIS data in near real time and which were developed at the VOLPE centre in the United States.

456. With one or two exemptions AIS data is gathered from the AIS systems of NATO member States.90 AIS data is also supplied to NATO by a number of other non-NATO States on the basis essentially of bilateral agreements.

457. The basic arrangement is that every State which supplies AIS data to the NATO MSSIS may receive raw or unprocessed AIS data that is received by NATO from the other participating States. There is no correlation between the volume of data supplied and that which can be received.91 The overall effect is that NATO has good global coverage.

---

90 The NATO Member States are Belgium, Bulgaria, Canada, Denmark, Estonia, France, Germany, Greece, Iceland, Italy, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Turkey, the United Kingdom and the United States. At present AIS data is not being provided by the Netherlands and Germany for legal reasons. It is understood that this situation will soon change. AIS data is provided by France in respect of its Mediterranean AIS stations in connection with Operation Active Endeavour but not those on the Atlantic.

91 In other words a country that supplies only 500 AIS tracks will nevertheless receive all of the tracks received within the MSSIS currently some 10,000.
458. NATO currently has two Maritime Component Commands, one in Northwood in the UK and the other in Naples, Italy. Each has a separate regional responsibility, MCC Naples being responsible for the Mediterranean and Black Sea in connection with the ongoing NATO Operation Active Endeavour, while MCC Northwood is responsible for the North Atlantic, North Sea and the Baltic. In addition a single Shipping Center is located at Northwood to maintain a global commercial shipping picture. Each MCC also has an MSSIS.

459. The result of this arrangement is that the location and movement of some 10,000 ships can be tracked each day. This creates a near real time picture of shipping activity as individual vessel tracks are on average three minutes old with no track older than 15 minutes. It is, however, a very complex picture which in itself is difficult to interpret.
460. The next step, therefore, is to analyse this mass of data in order to which vessels are a potential threat. This is done by running the raw data through a range of software analysis tools.

461. The principal tool is called BRITE (Baseline for Rapid Interactive Experimentation) which is essentially a database-analysis programme. BRITE is initially used to compare every AIS track with a range of open source databases, including Google, as well as commercial databases in order to identify anomalies. Such anomalies can include a non-existent or incorrect IMO number, the same IMO number being held by more than one ship, a mismatch between the IMO number and the name or call sign, etc, or a sudden and unforeseen change of course. Data is also held about ports so if a vessel claims to be heading to a port that cannot accommodate it due to its size such an anomaly will show up. Filters can also be applied to identify unusual events, such as ships meeting up at sea, or to follow the movement of vessels from specified countries.

462. Such analysis using open source data has the security level of ‘NATO unclassified’. It is not however shared with non-NATO states. Following the open-source data analysis, BRITE can also be run using classified intelligence information which may include data on individuals.

463. Individual ships may then be designated within three potential threat categories: (i) Critical Contact of Interest (CCOI); (ii) Contact of Interest (COI) and (iii) Vessel of Collection Interest (VOCI). A CCOI is a vessel on the maritime domain conducting activities considered to be an imminent threat to NATO, NATO nations and/or related assets and interests. A COI is a vessel conducting activities considered to be a potential threat to NATO, NATO nations and/or related assets and interests, while a VOCI is a vessel involved in any activity of intelligence interest. In other words vessels are designated as CCOI, COI or VOCI based on the assessed level of threat they pose to NATO.

464. Types of COIs and VOCIs include vessels in respect of which the owner or company is possibly associated with such activities as terrorism, the proliferation of weapons of mass destruction, irregular immigration, other illegal activity,
suspicious behaviour, environmental concerns and in certain circumstances vessels flying the flag of specific non-NATO Member States.

465. Apart from BRITE the other data analysis tools that are used are: ‘Fast2cap’, an alert provider that can be set up to identify specific actions, such as ships coming closer than 300 metres to a given platform or exceeding a specified speed, depending on operational requirements; and PANDA a new tool that will be tested in August 2008 in order to identify not only suspicious behaviour but also why such behaviour is suspicious. For example, an apparently suspicious significant route deviation may in fact be taken in order to avoid bad weather or a military exercise.

466. Once the MSSIS analysis is complete the relevant data is fed into NATO’s Maritime Command and Control Information System (MCCIS). Data held within the MCCIS is classified as in addition to containing the compiled picture created through MSSIS it also includes intelligence data, classified surveillance data (from satellites and other sensors) as well as the real time location of NATO assets (such as warships).

467. One of the reasons why the basic MSSIS is kept at an unclassified level, however, is in order to attract the participation of non-NATO States.

5.8.2 Legal basis
NATO is a defensive alliance that was established by the North Atlantic Treaty, which was signed on 4 April 1949 in Washington DC, as a bulwark against further Soviet expansion into Europe and the Atlantic region. A key feature of the North Atlantic Treaty is Article 5 which provides that an attack against one NATO Member State is an attack against all.92

The North Atlantic Treaty was subsequently supplemented by a range of additional legal instruments in order to create the relatively complex legal framework within which NATO currently operates. These include: (a) the Agreement on the Status of the North Atlantic Treaty Organisation, National Representatives and International Staff (Ottawa, 20 September 1951) (the Ottawa Agreement); (b) the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces (London, 19 June 1951)(the London Agreement); and (c) the Protocol on the Status of International Military Headquarters set up pursuant to the North Atlantic Treaty (Paris, 28 August 1952)(the Paris Protocol).

As far as the present discussion is concerned key issues that emerge from the Ottawa Agreement include the following:

- NATO possesses legal personality. In other words, NATO has the capacity to conclude contracts, to acquire and dispose of movable and immovable property and to institute legal proceedings;
- NATO, its property and assets, generally have immunity from every form of legal process except where waived;
- the premises of NATO are inviolable;
- NATO’s archives of NATO and all documents belonging to it or held by it are inviolable, wherever located;
- NATO has certain exemptions from taxation;
- no interference with NATO correspondence is permitted; and
- NATO international staff have certain privileges and immunities.

The London Agreement defines the status of forces when NATO States are sending and receiving troops as a genuine part of the co-operation within the alliance. In other words, it defines and governs the rights, responsibilities and jurisdiction of the “sending” State over its forces in another State of the Alliance and similarly the obligations, duties and jurisdiction of that “receiving” State.

The Paris Protocol, linked to the London Agreement, allows the provisions of that agreement to be applied, directly or tailored, to NATO International Military Headquarters.

92 The full text of Article 5 is as follows: ‘The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.’
As regards the acquisition and processing of surveillance data, maritime or otherwise, NATO does not have an explicit mandate, as such. Instead such activities are to be implied from the content of Article 3 of the North Atlantic Treaty which states:

In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.

In this connection it is also important to note the shift in emphasis of NATO’s operations following both the end of the so-called ‘Cold War’ and the terrorist attacks against New York on 11 September 2001. In particular under ‘Operation Active Endeavour’, which is conducted from MCC Naples and which was one of a number of measures taken following the invocation for the first time of Article 5 of the North Atlantic Treaty, NATO ships are patrolling the Mediterranean, monitoring shipping and providing escorts to non-military vessels through the Straits of Gibraltar to help detect, deter and protect against terrorist activity. The MSSIS plays a key role in supporting this ongoing Operation.

Furthermore, although combating human trafficking is not a primary focus of NATO the organisation nevertheless has a formal policy on this topic (which was adopted on 29 June 2004) and seeks to contribute as appropriate.

Finally, turning to the MMSIS itself, the exchange of AIS data with participating non-NATO Member States is governed by agreements between NATO and the recipient/s. These agreements may include the basis upon which information is shared, the level at which it is shared and the security protection afforded to that information. NATO considers that the protection of privacy and personal data is a significant concern and is aware that many member States and the EU have enacted laws and regulations intended to provide safeguards to personal data. Consequently NATO’s governing policy document on personal data protection (the NATO Joint Consultative Board Policy on Data Protection) is in general terms, similar to what most nations and the EU have enacted for information under their cognizance.

5.8.3 What data is shared?

In the context of MMSIS the data that is shared between NATO and non Member States is limited to raw AIS data.

5.9 Other planned data sharing mechanisms

Apart from the existing data sharing mechanisms described above, a number of new mechanisms are planned.

5.9.1 EUROSUR

The exchange of surveillance and other data is implicit in the scheme for the management of Europe’s external borders as provided for by the Schengen Border
Code. As already mentioned, Article 16(1) of the Schengen Border Code requires the Member States to ‘assist each other’ and to ‘maintain close and constant operation with a view to the effective implementation of border control…’. It goes on specifically to state: ‘They shall exchange all relevant information’.

480. Article 16(2) provides that the European Agency for the Management of Operational Cooperation at the External Borders of the Member States (‘FRONTEX’) is to be responsible for coordinating ‘operational cooperation between Member States in the field of management of external borders’. Article 11 of the Regulation pursuant to which FROTEX was established\(^\text{93}\) (the FRONTEX Regulation) provides that FRONTEX ‘may take all necessary measures to facilitate the exchange of information relevant for its tasks with the Commission and the Member States’.

481. On 13 February 2008 the European Commission adopted a Communication on the creation of a ‘European Border Surveillance System’ (EUROSUR), with the main purpose of preventing unauthorised border crossings, reducing the number of illegal immigrants losing their life at sea and increasing the internal security of the EU by contributing to the prevention of cross-border crime (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions examining the creation of a European Border Surveillance System (EUROSUR) hereafter the ‘EUROSUR Communication’\(^\text{94}\)).

482. Noting that some 50 authorities from 30 institutions in the eight Member States with external borders in the Mediterranean Sea are involved in border surveillance the EUROSUR Communication cites three main objectives: (a) the reduction of the number of illegal immigrants who manage to enter the EU undetected; (b) increase internal security of the EU as a whole by contributing to the prevention of cross border crime; and (c) enhancing SAR capacity.

483. The EUROSUR Communication, which drew on the findings of a number of earlier studies commissioned by FRONTEX proposes a phased approach to the creation of EUROSUR. It follows on from an earlier Communication of 30 November 2006 on Reinforcing the Management of the EU’s Southern Maritime Borders.\(^\text{95}\)

484. During the first phase as a first step it is proposed that existing surveillance systems and mechanisms should be interlinked and streamlined. A key element will be the establishment of a National Coordination Centres in the Member States that form the EU’s southern maritime borders in the Mediterranean and the southern Atlantic as well as the eastern land borders and the maritime borders in the Black Sea. The EUROSUR Communication states that:

\[
\text{Such centres should ensure close to real-time local, regional and national decision-making among all national authorities involved in border control tasks. Such centres should have the capacity to provide situational}\]


\(^{95}\) COM (2006) 733.
awareness of conditions and activities along the external borders as well as all the necessary tools to react accordingly.

485. It goes on to provide that they should function as the central part of the national border surveillance system.

486. The EUROSUR Communication next proposes, as a second step, the establishment of a secure computerised communication network in order to permit real-time data exchange 24 hours a day between centres in the Member States as well as FRONTEX. The third proposed step concerns the provision of support to third countries in the setting up of border surveillance infrastructure.

487. Phase 2 is concerned with the development and implementation of common tools and applications for border surveillance at EU level.

488. Of more relevance to this report is Phase 3 which is to focus entirely on the maritime domain. The Communication states that ‘objective of this phase is to integrate all existing sectoral systems which are reporting and monitoring traffic and activities in sea areas under the jurisdiction of the Member States and in adjacent high seas into a broader network, thus allowing border control authorities to take advantage of the integrated use of these various systems. This network constitutes also an aim of the integrated Maritime Policy of the EU’.

489. In other words this proposed policy initiative relates back to the present Study.

5.9.2 European Defence Agency - MARSUR

490. The European Defence Agency (EDA) was established pursuant to Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency96 (the EDA Joint Action).

491. The mission of EDA is specified in Article 2(1) of the EDA Joint Action as follows:

The mission of the Agency is to support the Council and the Member States in their effort to improve the EU’s defence capabilities in the field of crisis management and to sustain the ESDP as it stands now and develops in the future.

492. The acronym ESDP stands for the European Security and Defence Policy.

493. The functions and tasks of the EDA are specified in Article 5 of the EDA Joint Action which specifies that the EDA is to work in four principal fields:

- the development of defence capabilities in the field of crisis management;
- the promotion and enhancement of European armaments cooperation;
- working to strengthen the European defence industrial and technological base and for the creation of an internationally competitive European Defence Equipment Market; and
- the enhancement of the effectiveness of European Defence Research and Technology.

96 (OJ L 245, 17.7.2004 p 17)
494. The EDA began work on the Maritime Surveillance Project (MARSUR) some two years ago. The basic objective is to explore the needs and requirement for a purely European naval surveillance system. The MARSUR project is currently exploring the technical requirements of such a system and in this connection a draft feasibility study has recently been prepared that will contribute to the finalisation of a Common Staff Requirement.
6 Potential legal restrictions on sharing maritime monitoring and surveillance data

495. Having considered in detail the various European maritime monitoring and surveillance schemes this section contains a detailed analysis of the legal restrictions on data sharing and use. As if mirroring the complexity of the various schemes reviewed this is a complex area of law.

496. The focus of this Part is on potential restrictions imposed by international and EC law. Examples of potential restrictions deriving from the national legislation of a sample of Member States are described in a series of boxes that accompany the text. 97

6.1 Confidentiality of the data and commercial secrecy

497. The confidential nature of certain data can be a potential barrier to the exchange of such data. The confidentiality can originate from either legal provisions expressly stipulating that the data are confidential (or otherwise classified or protected by secrecy) or are to be treated in a confidential manner, or from contractual provisions to which the party holding the data needs to abide.

498. Examples of confidentiality can be found in certain maritime sector legal instruments described above, such as Article 14(2) of the VMS Regulation, Article 37 of the Control Regulation and Article 24 of the VTM Directive.

499. Contractual confidentiality restrictions can be found in relation to the supply of maritime information (such as AIS data) by commercial providers as discussed in more detail below.

6.1.1 Confidentiality of VMS data

500. With regard to the confidentiality of VMS data, reference should be made to Articles 3 and Article 37 of the Control Regulation.

501. Article 3 contains the legal obligation for Member States to establish a satellite-based vessel monitoring system (VMS) to monitor the position of Community fishing vessels (as further detailed in this Article). This means inter alia that Member States need to set up a fisheries monitoring centre (FMC) and to ensure that the FMC is equipped with computer hardware and software enabling automatic data processing and electronic data transmission and to keep computer files of the data for a period of three years.

502. It is explicitly provided (in Article 3(9)) that the Commission shall be granted access to these computer files on the basis of a specific request. It is further provided that Article 37 shall apply.

97 Examples are taken from Belgium, Finland, France, Germany, Greece, Malta, Spain and the United Kingdom.
Article 37(1) provides that ‘Member States and the Commission shall take all necessary steps to ensure that the data received in the framework of the Control Regulation shall be treated in a confidential manner’ (emphasis added).

Box B – Notions of professional secrecy in Member State law

The legislation of most Member States contains similar rules with regard to the duty of professional secrecy of government officials. Often a breach of these rules will be subject to criminal sanctions.

- In the UK, the Civil Service Code states that civil servants must not disclose official information without authority. It expressly states that the duty applies after civil servants leave the Civil Service. The Civil Service Code forms part of the contracts of employment of civil servants. Government officials could also be under a common law duty of confidentiality. Where confidential information is disclosed, in situations importing a duty of confidence, then it may be a breach of confidence to disclose that information. In addition, some types of information may be subject to the Official Secrets Act 1989, which covers information relating to security, intelligence, defence, international relations, etc. It is an offence, punishable by imprisonment, to disclose information in breach of the Official Secrets Act. Individuals will either automatically come within the Act by virtue of their job (e.g. working as a member of the security service) or will be told that the Act applies to them.

- In Germany, professional secrecy (Amtsverschwiegenheit) is an official duty of all civil servants and other public officials or employees of public authorities or institutions on federal, Länder as well as municipal level. Depending on the status of the respective person and the employing public authority, the legal basis of the duty is statute, collective agreement (Tarifvertrag) and/or employment contract. The general scope of the duty is basically identical. By way of example: “the employees are to observe secrecy with regard to any matters on which secrecy is required by statutory regulations or by the employer. The obligation continues to apply after termination of the employment contract” (Sect. 3 para. 1 of the Collective Agreement for the Public Service (Tarifvertrag für den öffentlichen Dienst, TVöD) of 13 September 2005). The duty is specified by different (internal) administrative regulations (Verwaltungsvorschriften) and also safeguarded by criminal law.

- In France, there is a general obligation of professional secrecy that applies to all civil servants (Article 26 of Act n°83-634 of 13 July 1983). The scope of the duty of secrecy to which civil servants are subject is very broad and covers all the information disclosed to civil servants in the course of their employment. In case of breach of professional secrecy, Article 226-13 of the French Criminal Code applies: “The disclosure of secret information by a person entrusted with such a secret, either because of his position or profession, or because of a temporary function or mission, is punished by one year’s imprisonment and a fine of €15,000”.

- In Spain, Article 53.12 of Act 7/2007 on the Basic Statute of Civil Servants, includes, among the general duties of officials of public bodies, the obligation to “keep secret of all classified information or of any other information the disclosing of which is legally prohibited, and shall keep due discretion in relation to any matters they are aware of as a consequence of its position, not being entitled to use the information obtained for their own benefit or for the benefit of third parties, or damaging the public interest”. The breach of the duties of secrecy and confidentiality may be subject to criminal sanctions under Article 417 of the Criminal Code.

- In Finland, the rules on “professional secrecy” applicable to government officials are stated in the Act on the Openness of Government Activities (621/1999, as amended). Pursuant to Section 23 of the Act, a person in the service of an authority and an elected official shall not disclose the secret content of a document, nor information which would be secret if contained in the document, nor any other information obtained in the service of the authority, where covered by a duty of non-disclosure provided in an Act. The provision on non-disclosure shall apply also after the service or the performance of the task on behalf of the authority has ceased. Section 24 of the Act further states that documents containing information on a private business or professional secret, as well as documents containing other comparable private business information, if access would cause economic loss to the private business (provided that the information is not relevant to the safeguarding of the health of consumers or the conservation of the environment or for the promotion of the interests of those suffering from the pursuit of the business, and that it is not relevant to the duties of the business and the performance of those duties), shall be secret.

- Also in Malta, officials and employees of the State are bound by professional secrecy, even after they cease to occupy the relevant office. Disclosure of professional secrets could lead to imposition of a fine or imprisonment.
According to Article 37(3), ‘the data exchanged between Member States and the Commission shall not be transmitted to persons other than those in Member States or Community institutions whose functions require them to have such access unless the Member States transmitting the data give their express consent’.

In addition, Article 37(4) stipulates that ‘the data communicated or acquired in whatever form by virtue of this Regulation is covered by professional secrecy and shall benefit from the same protection accorded to similar data by the national legislation of a Member State receiving them and by the corresponding provisions applicable to Community institutions’ (emphasis added). The Commission and the Member State FMCs are thus compelled to treat the VMS data in a confidential manner and can only disclose the data to persons in Member States or Community institutions on a “need-to-know” basis (unless the transmitting Member State consents otherwise).

VMS data communicated or acquired by the Member States’ FMCs and/or the Commission are thus to be considered as data that are covered by professional secrecy. In relation to professional secrecy, Article 287 of the EC Treaty provides that ‘the members of the institutions of the Community, the members of committees, and the officials and other servants of the Community shall be required, even after their duties have ceased, not to disclose information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components’.

It can be understood that the obligation to process the VMS data as confidential is due to the nature itself of the data which could indeed be seen as commercially valuable information and thus considered as commercially confidential by the operators of the fishing vessels concerned. In that respect, Article 3(3) of the initial proposal for the Control Regulation explicitly stipulated that ‘the Commission, the Member States’ competent authorities and officials and other agents are obliged not to divulge the data they gather pursuant to this Article and which are, by their nature, covered by business confidentiality’. However, there is no reason to conclude that the ‘duty of confidentiality’ should be seen as a legal barrier, as such, to the exchange of the data between the Commission and relevant Member States’ authorities or between Member States provided the conditions and restrictions laid down by Article 37 are duly complied with (and the data are treated by each recipient in accordance with their respective obligations of professional secrecy). Therefore, any future initiative aiming at a wider circulation of VMS data between Community institutions and Member States’ authorities will need to properly address the confidentiality issue and provide sufficient safeguards in that respect (e.g. by providing that any recipient of the data is under a duty of confidentiality with regard to these data).

Reference can further be made to Article 37(5) of the Control Regulation which prohibits the use of the VMS data ‘for any purpose other than that provided for in this Regulation unless the authorities providing the data give their express consent

98 COM/92/392final, OJ C 280/5.
99 A careful reading of the various provisions of Article 37 learns that Member States may not only be the transmitters of VMS data but also the recipients (e.g. Article 37 (4): (…) Member State receiving (the data) (…)” or (5): “(…) in the Member State of the authority receiving the data (…)”).
and on condition that the provisions in force in the Member State of the authority receiving the data do not prohibit such use or communication'. Member States can thus use the VMS data they receive for other purposes than monitoring fishing vessels provided the disclosing Member State expressly consents to such use (and the national rules of the receiving Member State are complied with). Prior consent of the disclosing Member State would also be required if the receiving Member State would intend to communicate the VMS data to persons whose function does not require access to the data (cf. Article 37(3)).

509. In addition, Article 37(6) explicitly provides that paragraphs 1 to 5 of Article 37 "shall not be construed as obstacles to the use of the data, obtained by virtue of this Regulation, in the framework of legal actions or proceedings subsequently undertaken for the failure to respect Community fisheries legislation. The competent authorities of the Member State transmitting the data shall be informed of all instances where such data are utilised for these purposes. This Article shall not prejudice the obligations pursuant to international conventions concerning mutual assistance in criminal matters". Regardless of the restrictions laid down by Article 37(1) to (5), Member States (and the Commission) may therefore use the data to legally enforce Community fisheries legislation (without the consent of the disclosing Member State, but with the obligation to inform such Member State).

510. Nevertheless, it appears from the VMS Regulation that, with regard to the free exchange of VMS data, data protection considerations will have to be taken into consideration as well. Article 37 of the VMS Regulation clearly contains a number of provisions which reflect data protection concerns\(^{100}\) and therefore may affect the exchange of VMS data where personal data would be involved, especially if such exchange would be envisaged for other than enforcement purposes.

511. In relation to the confidentiality of VMS data, reference should be also be made to Article 14(2) of the VMS Regulation which (in relation to “access to data”) provides that “the data received in the framework of this Regulation shall be treated in a confidential matter”.

512. As with Article 37 of the Control Regulation, there is no reason to consider that this provision constitutes an obstacle as such to the exchange of data between Member States (as set out in the Regulation – cf. Article 10) and between Member States and the Commission (cf. Article 14(1) of the VMS Regulation which requires Member States to provide the Commission, on specific request, with remote (online) access to the computer files containing the VMS data). However, any recipient of the VMS data under this Regulation (i.e. within the framework of the effective monitoring of the fishing activities of vessels) is under a duty of confidentiality with regard to these data (i.e. can not disclose the data to non-authorized persons outside the scope and purpose of the VMS Regulation).

513. The confidentiality of the VMS data itself is also explicitly referred to in the Commission’s Proposal of 23 November 2005 for a Directive amending the VTM Directive\(^{101}\) where the synergy between AIS and VMS is considered: “investigation

---

\(^{100}\) Article 37(2), (7) and (10) of the Control Regulation.

of the possibilities of integrating these systems should take account of the needs and requirements of controlling fishing fleets, particularly as regards the security and confidentiality of the data transmitted” (emphasis added)\textsuperscript{102}.

514. The explanatory memorandum to this proposal provides that the possibility of combining AIS functionalities with fisheries monitoring systems should be examined, but that “such development work must not compromise the aims and respective requirements of each of these systems, in particular the anti-collision function for AIS and the need to make possible the secure and confidential transmission of fisheries monitoring information” (emphasis added). The issue is also explicitly addressed in the European Parliament’s report on the proposal: “the confidentiality of fishing locations has traditionally been crucial for the fishing fleet and must be guaranteed under the relevant European legislation” (emphasis added)\textsuperscript{103}.

6.1.2 Confidentiality of data under the VTM Directive

515. A confidentiality provision, similar to the one in the VMS Regulation, can also be found in Article 24 of the VTM Directive which provides an obligation for Member States “to take the necessary measures” (in accordance with their national legislation) “to ensure the confidentiality of information sent to them pursuant to this Directive”. This “confidentiality of information” provision is part of Title IV of the VTM Directive (“Accompanying Measures”)\textsuperscript{104}.

516. The information sent to Member States pursuant to the VTM Directive concerns \textit{inter alia} VTS data, voyage data recorder (VDR) data, ship routing data, Hazmat data, port entry data and mandatory ship reporting data. The broad wording of Article 24 (“information sent to the Member States pursuant to this Directive“) may lead to the conclusion that also AIS data are covered by confidentiality. References to AIS are indeed included in Chapter I of the VTM Directive (“Ship reporting and monitoring“): as described above, Article 6 requires ships calling at Community ports to be fitted with an AIS, while Article 9 obliges Member States to provide themselves with the appropriate equipment and shore-based installations

\textsuperscript{102} Recital (6) of the Proposal (which became recital (8) in the Council’s aforementioned common position of 9 April 2008).
\textsuperscript{104} In the Commission’s initial proposal for the Directive, this provision was drafted as follows: “Member States shall take the necessary measures to ensure the confidentiality of information sent to them pursuant to this Directive, and must use such information only for the purposes of maritime safety and preventing pollution by ships” (Article 21, COM/2000/0802 final, OJ 120E of 24 April 2001).
to receive and utilize AIS data taking into account a necessary range for transmission of the reports\(^\text{105}\).

517. Again, there is no reason to conclude that the obligation for the Member States to ensure the confidentiality of the data constitutes, as such, a barrier to the exchange of the data between Member States and the Commission. In fact, the VTM Directive clearly provides that the Member States and the Commission shall cooperate in facilitating and enhancing the exchange of useful data in relation to the implementation of the Directive and the development of a Community vessel traffic monitoring and information system\(^\text{106}\).

518. However, as for the VMS data, the recipients of the data covered by the VTM Directive will be under an obligation to treat the data as confidential and will therefore in principle be unable to disclose the data to non-authorised persons outside the scope and purpose of the VTM Directive. Here also, any initiative aiming at a wider circulation of data under the VTM Directive will need to properly address the confidentiality issue and provide sufficient safeguards in that respect (e.g. by providing that recipients of the data will be under a duty to keep the data confidential).

519. The competent authorities\(^\text{107}\), port authorities and coastal stations to which the notifications pursuant to the VTM Directive should be made are to be designated by the Member States (Article 22(1) of the Directive). A list of these competent bodies is also to be published by the Member States and to be communicated to the Commission. The number of entities involved in the exchanging and sharing of data under the VTM Directive will thus in principle be limited to those entities designated by the Member States for that purpose. The duty of confidentiality would prohibit any sharing of the data by the designated authorities with non-competent (i.e. non-designated) bodies.

520. Furthermore, it should be noted that in the aforementioned report of the European Parliament on the Proposal of the Commission for a Directive amending the VTM Directive (see above, 514), rapporteur D. Sterckx repeatedly expressed the Parliament’s concern with regard to the confidentiality of the data covered by the VTM Directive, as well as with regard the potential misuse of AIS data for commercial ends (especially if combined with VMS data)\(^\text{108}\).

521. In relation to SafeSeaNet, the report states that “it is essential to ensure commercial confidentiality (…)”\(^\text{109}\). The Parliament also proposes to insert a new

\(^{105}\) However, paradoxically, it appears that AIS data, because of their transmission via open frequencies, can also (easily) be captured and processed by other actors, such as individual hobbyists or private companies using the data for commercial purposes (see also below, 501). This, of course, puts the explicit confidentiality obligation for Member States receiving AIS data in another perspective.

\(^{106}\) See, for instance, recital (17) and Article 23 of the VTM Directive.

\(^{107}\) “Competent authorities” is defined by Article 3 of the VTM Directive as “the authorities and organizations designated by Member States to receive and pass on information reported pursuant to this Directive”, while “port authority” means “the competent authority or body designated by Member States to receive and pass on information reported pursuant to this Directive”.

\(^{108}\) In its Common position of 9 April 2008 on the proposed Directive, the Council seems to reject most of these concerns (http://register.consilium.europa.eu/pdf/en/08/st05/st05719-ad01_en08.pdf).

paragraph into Article 24 of the VTM Directive (on “confidentiality of information”), as follows: “Member States shall, in accordance with their national legislation, prevent AIS and LRIT data transmitted by ships from being made available or used for purposes other than safety, security and the protection of the environment”. Again, the Parliament justifies its amendment by referring to “a considerable number of confidentiality issues for those involved” (in particular in relation to AIS and SafeSeaNet)\(^{110}\).

522. Specifically in relation to AIS data, it is also important to refer to paragraph 6 of Regulation 19 of Chapter V of SOLAS which provides that the AIS reporting requirements described in the preceding paragraph 2.4.5 “shall not be applied to cases where international agreements, rules or standards provide for the protection of navigational information”.

### Box C – Business confidentiality in Member State law

The concept of “business confidentiality” or “business secret” may be statutorily defined in certain Member States and/or developed in Member States’ case law.

- **In Germany**, the term "commercial or business secret" is not statutorily defined as such, but recognized by law and used in different statutes. According to settled case law, a commercial or business secret is understood as a fact in connection with a business undertaking, which is not publicly known or available but known only to a limited group of people and which the proprietor of the business undertaking wants to keep secret due to a legitimate economic interest (since the judgment of the Federal Court of Justice – Bundesgerichtshof – of 15 March 1955 – I ZR 111/53, GRUR 1955, 424). Commercial and business secrets are generally accepted and protected by different German laws. In particular, the unauthorized disclosure of such secrets is deemed a criminal offence according to the German Criminal Code (Strafgesetzbuch) or the Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb) if conducted by members of certain professions (e.g. public officials).

- **Also in Spain**, the term "commercial or business secret" is as such not statutorily defined, although certain legal provisions refer to it, for instance the the Act 3/1991 on Unfair Competition (Article 13) or the Spanish Criminal Code (Articles 278-280). Legal doctrine, based on case law, generally provides the following definition: the knowledge and information that are not known by the general public (and may not be known by a third party without a substantial financial and time cost) and which are necessary for the manufacture or commercialization of a product or service or for the organization and financing of a business, so that such knowledge or information provides to the business owner a competitive advantage.

- **In Finland**, the Penal Code defines "business secret" as a business or professional secret and other corresponding business information that a businessman keeps secret and the revelation of which would be conductive to causing financial loss to him/her or to another businessman who has entrusted him/her with the information. The Finnish Supreme Court (the judgements of which usually have the status of rule of law) has not (so far) given any judgments regarding the scope of the term “business secret” as defined in the Penal Code. The Act of Unfair Business Practices uses the (undefined) term “trade secret” (which is however understood to have the same meaning as the term “business secret” contained in the Penal Code).

- **In the UK**, the terms “business secret” and “commercial confidentiality” do not have a defined meaning. The term “trade secret” is often used in employment contracts and therefore discussed in breach of contract and breach of confidence cases.

- **Also in Greece**, the protection of “business secrets” or “commercial confidentiality” is as such not regulated by law.

523. A similar provision can be found in paragraph 20 of the AIS Guidelines which is entitled “Confidentiality” and concerns the manual entering of AIS data: “when entering any data manually, consideration should be given to the confidentiality of this information, especially when international agreements, rules or standards provide for the protection of navigational information”.

524. In Article 6(2) of the VTM Directive, this is addressed in the following way: “ships fitted with an AIS, shall maintain it in operation at all times except where international agreements, rules or standards provide for the protection of navigational information”.

6.1.3 Other examples of confidentiality of maritime reporting and surveillance data

525. Also under the Port Security Regulation, certain data are explicitly classified as secret or confidential. For instance, in accordance with Article 13(2) of the Port Security Regulation, Member States are under an obligation (as far as possible and in accordance with applicable national law) to treat as confidential any “information arising from inspection reports and answers of Member States when it relates to other Member States”.

526. Article 12 of the Port Security Regulation provides that the Commission (in accordance with its Internal Rules of Procedure) and the Member States (in accordance with their national legislation) shall take “appropriate measures to protect information subject to the requirement of confidentiality to which it has access or which is communicated to them”. Article 13(1) provides that certain data (inter alia inspection reports and certain Member State arrangements in relation to port security) are secret and shall not be published (without prejudice to the public right of access to Community documents, however – see below, 6.5).

527. The ship reporting requirements laid down by Article 6 of the Port Security Regulation (i.e. the provision of security information prior to entry into a Member State port), however, do not seem to be affected by a mandatory requirement of secrecy or confidentiality.

528. Furthermore, confidentiality is also referred to in Section 10 of Chapter V of SOLAS Regulation 19-1 on LRIT, where it is provided that Contracting Governments shall “recognize and respect the commercial confidentiality and sensitivity of any long-range identification and tracking information they may receive” (emphasis added). In addition, Contracting Governments are required “to protect the information they may receive from unauthorized access or disclosure”\footnote{111}.\footnote{111 Unlike AIS however, LRIT data will be transmitted via a closed satellite-based system. Private operators would thus in principle not be able to capture and process the data.}

529. The Schengen Acquis also contains various confidentiality provisions\footnote{112}.\footnote{112 See for instance the Decision of the Executive Committee of 14 December 1993 concerning the confidential nature of certain documents (SCH/Com-ex (93)22 rev., as amended), OJ, 22 September 2000.}

530. Also, the EUROSUR Communication addresses the issue of confidentiality in relation to the integration of existing sectoral reporting and monitoring systems into a broader network (a “system of the systems”): “special attention has to be given to the security of these systems and tools, ensuring appropriate confidentiality, integrity and availability”\footnote{113}.\footnote{113 EUROSUR Communication, at page 10.}
6.1.4 Contractual confidentiality

531. Restrictions relating to confidentiality could also be encountered in contracts with data suppliers imposing their data policies onto recipients. Typically, this might occur in situations where the relevant authorities acquire the data from third party commercial providers which request the execution of an appropriate license agreement. Such agreements usually impose various restrictions on the licensee in relation to the use of the data (mostly connected with a requirement to respect the confidentiality of the data and/or the intellectual property rights of the data supplier).

532. By way of example, reference can be made to Article 3 of the Bilateral Shipping Information Agreement of LRF (which is used *inter alia* for the provision of AIS Live data) according to which “shipping information”¹¹⁴ can be acquired from LRF and which provides:

> The Client accepts the Services are confidential (insofar as the same have not come into the public domain otherwise than by the act or default of the Client) and the Client shall not divulge the contents of the Services or any part thereof in any form to any third party other than as used in pursuance of the Client's business. Any alteration to the nature of the Client's business which involves the use of the information supplied under this Agreement must be agreed in writing by LRF. The Client agrees to take all reasonable precautions to prevent unauthorised access to the Services (including access to the Client's premises) and to ensure that its employees and agents do not divulge the contents of the Services to any third party.¹¹⁵

533. In addition, Article 7 of the agreement provides that, except as otherwise agreed in writing with LRF, the customer may not use the data to provide a service to a third party or for purposes other than those stated in Schedule 4 (“Permitted Use”, *i.e.* solely for the exclusive internal use of the customer in the ordinary course of its business).

534. Customers, such as public authorities, purchasing maritime data from LRF may therefore be contractually committed to keep these data confidential (insofar as they have not come into the public domain – which may be a controversial issue of its own¹¹⁶) and to not use the data for other than internal purposes. Data sharing with third parties will then be prohibited by way of contract and a breach of the relevant contractual obligations could expose the customer to a potential termination of the agreement and liability.

535. A further example of confidentiality and use restrictions with regard to maritime surveillance data is provided by the end user licence for CleanSeaNet. Through this licence the authorised satellite owners/operators grant the Coastal

---

¹¹⁴ It is understood that this is mainly AIS data.

¹¹⁵ The “Services” of LRF are described as the delivery of “shipping information in computer readable form and associated computer programs, program materials, documentation files and equipment more particularly described in Schedule 1”.

¹¹⁶ Commercial AIS providers seem to argue that AIS data is in the public domain (*i.e.* the radio spectrum) and therefore not subject to any reception or use restrictions. It cannot be excluded, however, that the interception (and further use) of personal or business radio transmissions by “unauthorised persons” could conceivably constitute an offence under the laws of certain countries. How the existing national legislation will be applied may depend on the individual circumstances of the case (including the legality of the receiving device in the place of receipt), as well as on a number of qualification issues, such as “private versus public communication network” or “private versus public communication service” or the scope of the “communication secret”.
States via EMSA a “limited, non-transferable, non-exclusive license to use the Product and any accompanying written materials provided to the Coastal State by EMSA and any Derived Image Product”, solely for a number of specified uses, such as the transfer “via either a physical delivery protocol or a secured and encrypted network protocol” of a full resolution product to the Coastal States’ officials and/or contractors or consultants “who are under a duty of confidentiality no less restrictive than (the Coastal State’s) duty hereunder” (emphasis added).

536. Furthermore, the CleanSeaNet end user licence contains a number of restrictions and prohibitions with regard to the use of the data, as well as a clear purpose-limitation: “the Products shall be used for the sole purpose of oil spill monitoring (illegal discharges and accidental spills)”\(^\text{117}\). A use of the data for other purposes than oil spill monitoring would therefore be prohibited by the licence agreement.

537. Typically, data supply agreements of this type will also include provisions on the protection of the data supplier’s intellectual property rights, such as database rights\(^\text{118}\) or copyright (e.g. on photographs or other images), which the customer will need to comply with. However, there is no reason to conclude that these intellectual property claims might constitute, as such, a barrier to the exchange of maritime reporting and surveillance data, as long as the related contractual provisions on intellectual property rights are complied with by the recipient of the data (for instance, as long as the copyrighted data are not reproduced or distributed without the prior consent of the rights holder).

538. By way of example, reference can be made to Article 2 of the LRF Agreement which provides that “the copyright and other intellectual property rights in the Services and all programs, files and other documents prepared by LRF in connection with this Agreement are and will at all times remain the property of LRF (…)”.

539. The licence conditions available on the website of AISLive, the online data service operated by LRF, require the subscribers to “acknowledge that AISLive and its third party providers own all right, title and interest in and to the System, including but not limited to all data and content therein and all associated intellectual property rights. Nothing herein shall be deemed a transfer of any such ownership rights to you”\(^\text{119}\).

540. Also, the CleanSeaNet end user licence conditions provide that “no license or right in or to any of the Products, or any other intellectual property of the

---

\(^\text{117}\) The full text of the licence is available at [http://cleanseanet.emsa.europa.eu/About/end_user_license.html](http://cleanseanet.emsa.europa.eu/About/end_user_license.html).

\(^\text{118}\) Databases (i.e. collections of data arranged in a systematic or methodical way) are accorded copyright protection under EU and Member States’ law (cf. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77 of 27 March 1996, which in addition also provides the maker of a database with a *sui generis* right that prevents the unauthorised extraction and/or re-utilisation of the whole or a substantial part of the database where the maker shows a substantial qualitative and/or quantitative investment in obtaining, verifying or presenting the contents of the database).

\(^\text{119}\) [http://www.aislive.com/licence.html](http://www.aislive.com/licence.html): the “System” is defined as “the AIS Live Ltd AISLive.com system as may be amended by AISL from time to time and accompanying software”. Similar provisions can be found in the licence conditions for Sea-Web, another LRF service available on the internet: [http://www.sea-web.com/licence.html](http://www.sea-web.com/licence.html) (Sea-Web is an online register of ships).
authorised satellite owners/operators or EMSA, is granted by this License’. The governmental organisations of Coastal States are required to always conspicuously display the copyright notice of the satellite owner and EMSA alongside the satellite images. The licence conditions also explicitly provide that “the identified authority or authorities of the Coastal States may not distribute, transfer or otherwise make available the Product to any subsidiary, affiliate or other governmental bodies, or any other unauthorised users, without the prior written consent of EMSA” (emphasis added).

541. Therefore, if Community or Member State authorities source maritime reporting or surveillance data from commercial third party suppliers (such as LRF), they may have to take into account contractual conditions potentially restricting their ability to freely share the acquired data with other recipients (i.e. use restrictions or prohibitions, non-disclosure or confidentiality obligations, or intellectual property claims of the data supplier). As a consequence, the further sharing of any such data may be subject to the prior consent of the supplier of the data. Such consent will be implied where designated competent authorities would be legally authorised or compelled to share the data they are controlling.

### 6.2 Processing of personal data

#### 6.2.1 Relevant legal framework

542. Another potential restriction on data sharing may be linked to the nature of the data itself. In cases where maritime reporting and surveillance data involves personal data, data protection laws will in principle become applicable (subject to exceptions). This may constitute a significant barrier to the (unrestricted) exchange of the data (or will at least require the necessary safeguards to be put in place for the data sharing to be allowed).

543. The exact scope of the concept of “personal data” will of course be crucial to assess whether any such data are involved in the various reporting and surveillance systems described in this Study. This will be examined below.

544. The two main instruments of European Community data protection law are:

(i) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (‘the Data Protection Directive’)\(^\text{120}\); this Directive applies to the processing of personal data by natural persons, legal persons and public authorities in the Member States; and

(ii) Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (‘the Data Protection Regulation’)\(^\text{121}\);

\(^{120}\) OJ L 281/31 of 23 November 1995.

this Regulation applies to the processing of personal data by Community institutions and bodies (in so far as such processing is carried out in the exercise of activities all or part of which fall in the scope of Community law)\textsuperscript{122}.

545. The rationale for the Data Protection Directive is that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals (notably the right to privacy\textsuperscript{123}) should be safeguarded and protected, specifically with respect to the (automated or otherwise systematic) processing of any personal information\textsuperscript{124} that relates to them. In brief, data protection law aims to establish conditions under which it is legitimate and lawful to process personal data and obliges data controllers to respect a number of rules and principles. It also empowers data subjects by granting them a number of rights in relation to the processing of their data and provides for supervision by independent authorities.

546. The differences in the level of protection of the rights and freedoms of individuals in the Member States were seen as obstacles to the transmission of personal data from one Member State to another and, as such, as affecting not only economic activities within the Community but also the duties and tasks of national authorities where Community law requires them to collaborate and exchange personal data with other Member States' authorities within the context of the internal market\textsuperscript{125}.

547. Therefore, the Data Protection Directive aimed at an approximation of national laws in the field of data protection. The idea is that the level of data protection should be equivalently high in all Member States so that Member States are no longer able to inhibit the free movement between them of personal data on grounds relating to the protection of the rights and freedoms of individuals and in particular the fundamental right to privacy.

548. The aim of the Data Protection Regulation is to make the general principles of the Data Protection Directive also binding for the Community institutions and bodies. The principles laid down by both instruments are therefore largely similar.

549. In addition, consideration should be given to specific data protection provisions included in other legislation. Some examples for the maritime sector will be referred to below.

\textsuperscript{122} The Regulation thus applies to the European Commission, but also to subordinated agencies such as the European Maritime Safety Agency (EMSA).

\textsuperscript{123} The right to privacy is recognised in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and is also part of the general principles of Community law (cf. Article 6 of the EU Treaty) and of the Constitutional laws (and traditions) of many States. Article 8 of the ECHR provides that “everyone has the right to respect for his private and family life, his home and his correspondence” and that “there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

\textsuperscript{124} Such information can range from simple contact details over salary information, ID numbers, banking details or credit status to “sensitive” information such as data concerning race, religion, health or sex life.

\textsuperscript{125} Recitals (5) and (7) of the Data Protection Directive.
550. Reference also needs to be made to the opinions, recommendations and guidelines published by: (i) the various independent data protection supervisory authorities which were established in each Member States pursuant to Article 28 of the Data Protection Directive; and (ii) the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (‘the Article 29 Data Protection Working Party’ or ‘the Article 29 WP’), which advises the European Commission on data protection matters.

551. The processing of personal data by Community institutions and bodies is also supervised by an independent supervisory authority, the European Data Protection Supervisor (hereinafter ‘the EDPS’), pursuant to Article 41 of the Data Protection Regulation.

6.2.2 The broad concept of personal data

552. The concept of “personal data” (but also of “processing”) is very broadly defined in the Data Protection Directive (with definitions being identical in the Data Protection Regulation).

553. Article 2(a) of the Data Protection Directive defines “personal data” as “any information relating to an identified or identifiable natural person (‘data subject’)” (emphasis added). The definition further specifies that “an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (emphasis added).

554. This very broad definition of personal data has lead to uncertainty and diversity in practice among Member States which was felt to undermine the proper functioning of the data protection framework. The Article 29 WP has therefore (recently) issued guidelines in order to come to a common understanding of the concept of personal data throughout the EU.

555. In its Opinion on the concept of personal data, the Article 29 WP thoroughly examines the four components of the definition of personal data: (i) any information, (ii) relating to, (iii) an identified or identifiable, (iv) natural person.

---

126 For instance, the Commission Nationale de l’Informatique et des Libertés (CNIL) in France or the Information Commissioner in the UK.

127 The Article 29 WP is established by Article 29 of the Data Protection Directive and is composed of representatives of the Member States’ supervisory authorities.


129 The Data Protection Directive does in principle not cover the protection of legal persons with regard to the processing of data which concerns them. However, the European Court of Justice has made clear that nothing prevents the Member States from extending the scope of the national legislation implementing the provisions of the Directive to areas not included within the scope thereof, provided that no other provisions of Community law preclude it (judgement of the European Court of Justice C-101/2001 of 6 November 2003, Lindqvist). Accordingly, some Member States have extended the application of certain provisions of national law adopted pursuant to the Data Protection Directive to the processing of data on legal persons. In the Opinion 4/2007 of the Article 29 Data Protection Working Party of 20 June 2007 on the concept of personal data (WP 136), reference is notably made to Luxembourg, Italy and Austria (p. 23 – 24).
556. What is of interest for this Study on maritime reporting and surveillance data is that the Article 29 WP confirms that particular pieces of information such as “a telephone number, a car registration number, a social security number, a passport number” can be sufficient to render someone directly or indirectly identifiable. The extent to which these identifiers are sufficient to effectively achieve identification is something that will depend on the context of a particular situation.

557. In addition, it is important to note that, in certain circumstances, information on legal persons can also constitute personal data, for instance where the name of a legal person derives from that of a natural person (e.g. an undertaking bearing the name of its owner). There may therefore be circumstances where data about a legal person can legally qualify as data relating to a natural person.

558. An example can be found in the recent opinion of the EDPS on the Proposal for a Regulation establishing common rules concerning the conditions to be complied with to pursue the occupation of road transport operator. In that opinion, the EDPS points out that road transport undertakings can also be natural persons, in which case the processing of data on these undertakings (e.g. in a register) falls within the scope of data protection law. It is felt that the same reasoning could apply to maritime undertakings (vessel owners) if they would appear to be natural persons. Therefore, any information collected or transmitted via a maritime surveillance or reporting scheme that could lead (directly or indirectly) to the identification of that undertaking/natural person will have to be considered as “personal data” and may thus be affected by the restrictions of data protection law.

559. Consequently it seems reasonable to conclude that the name of a vessel may as such not be sufficient to directly identify the (natural) person(s) owning the vessel. However, it may be possible that this person can be indirectly identified through the unique combination of the name of the vessel with other data elements (whether retained by the data controller or not), e.g. the unique registration number of the vessel. Although at first sight appearing as purely “object-related” or “activity-related”, data such as the name or registration number of a vessel may therefore constitute “personal data” in the meaning of the Data Protection Directive (and Data Protection Regulation), if it is possible to single out a particular person on the basis of those data (i.e. the natural person owning the vessel, the captain of the vessel, crew members, …).

560. It is also important to note that pictures or CCTV images (or other visual data) are generally to be considered as personal data, if it is possible to identify natural persons on the images. Recital (16) of the Data Protection Directive, however, specifically provides that the processing of sound and image data (for instance, video surveillance) does not come within the scope of the Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law. However, any filming of vessels or other maritime activity (that could lead to the identification of persons) for purposes other than the aforementioned will in principle have to comply with data protection law.

---

130 OJ C 14/1 of 19 January 2008.
Box D – The scope of ‘personal data’ in Member State law

- In Belgium, the Privacy Commission has ruled that a purely object-related piece of information such as a chassis number is a unique identification number as it allows the identification of a vehicle throughout its lifecycle. The fact that this number is unique makes it practical for combination with other data which could lead to the identification of a person (i.e. the owner of the vehicle or the holder of the car number plate). In that respect, the chassis number can become personal data in the meaning of the Data Protection Directive 131.

- In Finland, the Data Protection Ombudsman has ruled that a vehicle registration number is considered as personal data if the registrar has the information, or he contemplates to acquire information, on who (recognisable data subject) can be connected to the respective vehicle registration number (i.e. the owner of the vehicle or the holder of the vehicle registration number).

- It is very likely that several other national data protection supervisors have ruled or would rule in the same sense. This is the case, for instance, with the CNIL in France which also interprets the notion of “personal data” very broadly. In the UK, there has been some debate as to whether vehicle registration numbers (i.e. number plates) should be personal data, but no guidance or decision has been issued on this (although it seems likely that the Information Commissioner would consider this to be personal data if combined with other information, e.g. about the vehicle’s owner).

- In Germany, the Constitutional Court recently decided that different Länder statutes governing the automatic recording of car number plates were unconstitutional as they violate privacy rights. The respective legal provisions lacked a clear definition as to when data may be collected and of the scope of data use.

Box E – National variations in implementation measures

561. Taking the above into consideration, the detailed analysis of the data collected and transmitted in most of the maritime reporting and surveillance systems described in this Study leads to the conclusion that these data could potentially involve personal data (e.g. where the reporting or surveillance concerns a fishing vessel identification number, a licence number, an external registration or side number or other unique identifiers that can lead – directly or indirectly – to the identification of a natural person). This will obviously also be the case where names or addresses of persons have to be reported (crew lists, passenger lists etc.).

562. Where, in the large majority of cases, the vessel owner or agent will be a legal person, this may not necessarily always be the case. If the vessel owner or agent is a natural person, the data that could lead to his identification (directly or indirectly) are to be considered as personal data 132. Furthermore, the widespread use of AIS B for pleasure craft may lead to the introduction of personal data into AIS networks as pleasure craft are much more likely to be owned by individuals.

---


132 It is reiterated here that some Member States have extended the scope of their data protection laws to include legal persons as well.
As with basically any Directive, local variations may exist in the implementation measures of the Data Protection Directive throughout the Member States (although usually not with regard to the general principles laid down by the Directive). In addition, local data protection supervisory authorities may have issued differing opinions on specific data protection issues, while national courts may also have given different interpretations to some of the principles laid down by data protection law.

For instance, in the UK, there seems to be a difference in opinion with regard to the exact scope of the concept of “personal data”. UK case law has interpreted the definition of personal data narrowly. Significantly in the case of Durant, the Court of Appeal stated that information must be “biographical in a significant sense”, i.e. going beyond the fact that an individual was involved in a matter or event. Additionally, it must have the data subject as its focus in order to be personal data. In light of the aforementioned Article 29 WP’s opinion on personal data, the UK data protection supervisor (the Information Commissioner) issued revised guidance on what is personal data. Although this guidance refers briefly to the Durant case, the approach is consistent with the Article 29 WP’s opinion. However, due to the rules of precedence in the UK, courts will have to follow Durant in assessing what is personal data.

In Germany, the interpretation of the term “personal data” generally corresponds to that of the Article 29 WP. However, the term “identifiable” is not defined by the German Data Protection Act (Bundesdatenschutzgesetz) and, apparently, the interpretation of that term may differ, in particular in case of indirect identification. The term “identifiable” is generally understood in a relative way. There have been different court decisions and opinions of data protection supervisors regarding the quality of certain data as personal data, in particular with respect to the question of identifiability. For the determination of the identifiability, only the knowledge and means of the data controller determine whether or not a person will be considered as identifiable. That means that data may qualify as personal data for one user of the data, whereas it is considered anonymous and therefore not “personal” for another user. Whenever data allows the controller to identify the individual, directly or indirectly (e.g. by combining different pieces of information), the data will be considered personal data. Thus, the applicability of data protection law may deviate in particular cases. In view of the Article 29 WP’s Opinion on the concept of personal data, it is unclear if the interpretation of the term “identifiable” will be upheld in the future.

In France, the term “personal data” is very broadly construed. The definition provided in Article 2 of the Data Protection Act n° 78/17 of 6 January 1978 is even slightly broader than the definition given in the Data Protection Directive as it provides that “in order to determine if a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration”. As a consequence, any data that can lead to the identification of a person, even if the data controller does not have the necessary information to identify the person as long as anyone may have this information, constitutes personal data.

In Spain, the term “personal data” is substantially in line with the definition of the Data Protection Directive as well as with the interpretation of the Article 29 WP. However, Spanish data protection contains certain particularities in relation to the specific question of the applicability of the term “personal data” to businesses. Articles 2.2 and 2.3 of the Secondary Regulation Implementing Organic Act 15/1999 on the Protection of Personal Data provide that (i) the data protection rules “shall not be applied to data processing regarding legal entities, nor to the files that only record data of individuals providing services in them, comprising only their name and surname(s), functions or jobs performed, as well as the postal or e-mail address and professional telephone and numbers”, and (ii) “similarly, data relating to sole traders, when referring to them as traders, industrialists or ship owners, shall also be excluded from application of the system of protection of personal data”.

133 Durant v Financial Services Authority [2003] EWCA Civ 1746. Mr Durant had requested information relating to a complaint he had made to the UK Financial Services Authority (FSA) about his bank. The Court of Appeal held that the information was not personal data, as Mr Durant was not the focus of the information requested (the court held that the focus of the information was the complaint and the objects of those complaints, e.g. the FSA and the bank).

134 In view of the doctrine of precedent, until Durant is overruled by the House of Lords, all other courts will have to follow the decision. This has been seen recently in a Freedom of Information case (the Yorkshire forward case) where the Information Tribunal looked at both Durant and the Information Commissioner’s guidance on the concept of personal data. The Information Tribunal stated that “we have difficulty in reconciling the approach in the Guidance with that in Durant”. The Tribunal followed Durant in stating that information had to be significant biographical information to amount to personal data. It held that a list of attendees at a conference was not personal data as it was not biographically significant.
From various legal instruments in relation to maritime reporting and surveillance systems, it appears that data protection concerns were taken into consideration from the outset.\(^{135}\)

For instance, Article 15 of the Framework Regulation (which is concerned with fishing fleet registers) provides that the Commission shall comply with the Community provisions regarding the protection of personal data when setting up (and making available) a Community register.

Article 11 of the Register Regulation (on access to the Community fishing fleet register) explicitly provides that Member States’ access to the register needs to take place in compliance with the Data Protection Regulation, and in particular with Article 8 of this Regulation which provides that Community institutions and bodies can only transfer personal data to other recipients if these recipients (e.g. Member States’ competent authorities): (i) establish that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority; or (ii) establish the necessity of having the data transferred (and there is no reason to assume that the data subject’s legitimate interests will be prejudiced).

It is further provided in Article 11 of the Register Regulation that the public shall be granted access to a version of the register which does not contain personal data.

In addition to the confidentiality of the data (described above), Article 37 of the Control Regulation also addresses the issue of the protection of personal data in a very broad way. Article 37(2) prohibits the transmission of (VMS) data that would allow “the direct or indirect identification of natural or legal persons” (emphasis added).\(^{136}\)

It also prohibits the transmission of names of natural or legal persons to the Commission or to other Member States if not expressly provided for in the Regulation or if not necessary for the purposes of preventing or pursuing infringements or the verification of apparent infringements under the Control Regulation. Article 37(9) provides that (VMS) data shall only be stored in a form “allowing the identification of the persons concerned” for as long necessary for the fulfilment of the purposes in question.\(^{137}\)

Article 3(1)(2) of the Schengen Borders Code also contains an explicit reporting requirement involving personal data (i.e. requirement to provide the

---

\(^{135}\) It is to be noted that also LRF, in its proposed licence agreement for the online register of ships Sea-Web, explicitly addresses the issue of data protection (http://www.sea-web.com/licence.html).

\(^{136}\) It is reiterated however that Article 37(6) explicitly provides that paragraphs 1 to 5 of Article 37 shall not be construed as obstacles to the use of (VMS) data in the framework of legal actions or proceedings undertaken for the failure to respect Community fisheries legislation (see above, 479). Regardless of the data protection restrictions laid down by Article 37(1) to (5), Member States (and the Commission) may thus use the data to legally enforce the Community fisheries legislation (without the consent of the disclosing Member State, but with the obligation to inform such Member State).

\(^{137}\) See further also Article 37(7) “(...) the data stored in a form allowing identification of the person concerned shall be deleted without delay”, or Article 37(10): “the data received in the framework of this Regulation shall be available upon request to the natural or legal persons concerned".
Similar provisions can be found in the Port Security Regulation\textsuperscript{138}.

\begin{box}
\textbf{Box F – References to data protection concerns in maritime sector instruments}

Also at Member State level, examples can be found of legal instruments in the maritime sector that specifically address data protection concerns. For instance in Germany, the maritime and fisheries sector is subject to a vast number of statutory laws at federal and Länder level which generally contain provisions concerning the collection and use of (personal) data by the competent public authorities with respect to their rights and duties under the respective statute. In some cases, the scope of admissible use of personal data is determined by the principles of the German Data Protection Act (GDPA) as the general statute regarding data protection. In other cases, the respective statute contains specific provisions that may vary from or specify the scope of the general principles. However, these laws do not generally allow the exchange of personal data. Rather, such exchange is either expressly specified as admissible or it would have to meet the requirements under the GDPR.

In particular, the \textbf{Maritime Responsibilities Act} (\textit{Seeaufgabengesetz}) appears to be of relevance. This Act regulates the duties and functions of the Federal government regarding aspects on maritime matters, including maritime safety and security on coastal waters, vessel traffic, the collection and use of data on vessels, their owners and crew. The types of data which may be collected and used for the performance of duties and tasks under the Maritime Responsibilities Act are specified in Section 9. The data includes potential personal data, e.g. identification data of the crew and owner, vessel name, vessel number, position data. According to Section 9e §1 s.2, the data may be collected by means of automated vessel identification systems or the voyage data recorder, unless military vessels are concerned. The Act contains explicit provisions regarding the transfer of such data to other public authorities, such as other national security authorities (e.g. coast guard, border patrol, customs), international authorities or organisations (e.g. IMO, EMSA), as well as private bodies (e.g. port operators). It is provided that any such transfer is only admissible if the recipient requires the data in order to fulfil its own duties.

The recent “legal history” of Section 9e\textsuperscript{139} of the Maritime Responsibilities Act (it was introduced into the Act in April 2008) is also particularly interesting in the light of this Study. In the Federal Government’s official reasoning for introducing this new provision\textsuperscript{140}, it is specified that until 2004 there had already been a provision on data protection in the Act (also in Section 9e), but it had been removed as it was believed that all data protection issues were duly covered by the GDPA. However, the experience in the following years demonstrated that the abolishment of this provision entailed specific legal issues justifying the re-introduction of a specific provision dealing with the collection and sharing of personal data in maritime matters. These issues specifically concerned the sharing of data by the maritime authorities (e.g. shipping administration) with security and police agencies for border control purposes, as well as the sharing of data with private companies (such as port operators). Specific reference is also made to the participation in the worldwide database “IMO Unique Company and Registered Owner Identification Number Scheme” operated by the private company Lloyd’s Register-Fairplay (LRF). It is also interesting to note that §1 s.3 of the newly introduced Section 9e explicitly deals with the sharing of data with foreign institutions such as IMO, EMSA and the Equasis database. This provision basically aims to ensure that, in such circumstances, the German data protection standards are maintained. Exceptions are made with regard to serious breaches of international rules on shipping security or maritime environmental protection and as regards the transfer of data within the framework of activities which are fully or partly falling within the scope of Community law.

The Agreement on access to AIS information, developed by the Working Group of HELCOM, also explicitly takes into account the issue of sharing “information concerning private persons” by providing that “when AIS-data contain information concerning private persons the Participating parties undertake to ensure protection of the privacy of these persons in accordance with the Directive 95/46/EC on the protection of individuals with regard to the processing of

\textsuperscript{138} See section 4(41) of Annex III of the Port Security Regulation.

\textsuperscript{139} A translation of Section 9e of the German Maritime Matters Act is attached as AnnexC.

\textsuperscript{140} Gesetzentwurf der Bundesregierung - Entwurf eines Gesetzes zur Änderung seeverkehrsrechtlicher, Verkehrsrechtlicher und anderer Vorschriften mit Bezug zum Seerecht; Bundestagsdrucksache 16/7415 of 5 December 2007.
personal data and on the free movement of such data and also to other applicable international, European Community and national law and regulations”.

571. The EUROSUR Communication also addresses the issue of the protection of personal data in relation to the proposed integration of existing sectoral reporting and monitoring systems into a broader network: “The different activities referred to in the previous sections may involve the processing of personal data. Thus the principles of personal data protection law applicable in the European Union are to be observed, meaning that personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The processing of personal data within the context of EUROSUR must therefore be based on appropriate legislative measures, which define the nature of the processing and lay down appropriate safeguards” (emphasis added).

572. Finally, it is to be noted that, from a data protection point of view, the way in which data are transmitted (e.g. in a secured point-to-point way or via open frequencies) does not, as such, affect the nature of the data: if the data fall within the defined scope of the concept of “personal data”, the provisions of data protection law will in principle become applicable and will have to be complied with by those controlling and processing the data.

6.2.3 The broad concept of processing of personal data

573. In addition to the very broad concept of “personal data”, there is also the broad definition of the concept of “processing of personal data”.

574. Both the Data Protection Directive and the Data Protection Regulation apply to “the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system”.

575. “Processing” is defined by both the Data Protection Directive and the Data Protection Regulation as “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.

576. The definition of “processing” is thus extremely broad and basically covers any type of manipulation of data that can be considered as personal data. Certainly it covers the type of collection, recording and storage of data in a database or register,

141 The HELCOM Agreement on access to AIS information (as amended) is available on: http://www.helcom.fi/stc/files/Krakow2007/Amendment%20to%20the%20HELCOM%20AIS%20Agreement.pdf.
142 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions examining the creation of a European Border Surveillance System (EUROSUR), COM/2008/68 final of 13 February 2008, p. 11.
143 Article 3 (1) of the Data Protection Directive and Article 3 (2) of the Data Protection Regulation; “filing system” is defined as “any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis”.
144 Article 2 (b) of the Data Protection Directive and of the Data Protection Regulation.
as well as the disclosure, transmission or exchange of personal data with other recipients, as described in this Study.

577. As the reporting and surveillance systems described in this Study may involve the processing of personal data (not least in jurisdictions where the scope of data protection law extends to legal persons), it needs to be examined what are the main restrictions on the sharing of these data from the standpoint of data protection law.

578. In that respect, the principle of proportionality and purpose-limitation should probably be mentioned as potentially one of the main restrictive factors.

6.2.4 The principles of proportionality and purpose-limitation

579. One of the cornerstones of data protection law is the purpose-limitation: personal data can only be processed for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.\(^{145}\)

580. In addition, the processing of personal data must be adequate, relevant and not excessive “in relation to the purposes for which they are collected and/or further processed”\(^{146}\) (principle of proportionality).

581. Personal data can thus, in principle, not be processed for purposes other than the purposes for which they were collected. A clear and precise description of the purposes of the data processing is therefore of crucial importance. In the same way, it needs to be clearly defined who is the data controller, i.e. the person responsible for the processing of the data and thus for compliance with data protection law.\(^{147}\)

582. From the perspective of data protection law, the processing of personal data needs to remain restricted to: (i) the competent authorities (data controllers) designated for such processing; and (ii) the purposes laid down by the relevant laws or regulations that allow (or impose) the processing.

583. Examples of the purpose-limitation for data processing can also be found in the maritime sector legislation.

584. For instance, Article 13(1) of the VMS Regulation provides that Member States shall use the data received “for the effective monitoring of the fishing activities of vessels”, while Article 37(5) of the Control Regulation prohibits the use of VMS data “for any purpose other than that provided for in this Regulation unless the authorities providing the data give their express consent and on condition that the provisions in force in the Member State of the authority receiving the data do not prohibit such use or communication”. A use of VMS data for purposes other than

\(^{145}\) Article 6 (1) (b) of the Data Protection Directive; Article 4 (1) (b) of the Data Protection Regulation.

\(^{146}\) Article 6 (1) (c) of the Data Protection Directive; Article 4 (1) (c) of the Data Protection Regulation.

\(^{147}\) “Data controller” is defined as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.” Where the purposes and means of the processing are determined by Community law or national laws or regulations, the controller (or the specific criteria for his nomination) may also be designated by Community or national law (Article 2(d) of the Data Protection Directive; cf. also Article 2(d) of the Data Protection Regulation).
those for which they were received would therefore require the express consent of
the Member State disclosing the data.

585. Specifically with regard to the sharing of (personal) data through the linking of
databases (or access to these databases) between Member States and between
Member States and Community institutions, the EDPS has issued several
interesting opinions. The general principles (and concerns) of the EDPS with
regard to data sharing can be summarized as follows:

(i) if access is granted to a third party database or system, the tasks for which
such access is granted must be consistent with the purposes of the database
or system (no unlimited, systematic or routine access)\textsuperscript{148};

(ii) the exchange of data must be limited to what is necessary for the purpose of
the processing and as far as this is in proportion with the purpose (the EDPS
clearly speaks out against the interoperability of databases or systems if this
would infringe the principle of purpose-limitation);

(iii) making databases or systems directly accessible by third party authorities
means an increased number of persons having access to the data and thus a
growing risk of misuse of the data; therefore, a clear description is needed
of the designated authorities (and authorized persons) that will have access
to the data (with the drawing up and publication of a list of such
authorities)\textsuperscript{149};

(iv) granting \textit{direct} access to databases and systems creates issues of control:
the controller of the database or system has no control over the access to
and further use (e.g. the interpretation) of the data by the third parties who
access them, neither will the controller be able to ensure and control the
accuracy of the data\textsuperscript{150} once they have been accessed by a third party\textsuperscript{151}.

\textsuperscript{148} See, for instance, Opinion of the European Data Protection Supervisor of 23 March 2005 on the
Proposal for a Regulation of the European Parliament and of the Council concerning the Visa
Information System (VIS) and the exchange of data between Member States on short stay-visas, \textit{OJ C} 181/13, and Opinion of the European Data Protection Supervisor of 20 January 2006 on the Proposal for
a Council Decision concerning access for consultation of the Visa Information System (VIS) by the
authorities of Member States responsible for internal security and by Europol for the purposes of the
prevention, detection and investigation of terrorist offences and of other serious criminal offences, \textit{OJ C} 97/6.

\textsuperscript{149} For instance, the VMS Regulation contains a list of “competent authorities” (Annex II), \textit{i.e.}
the Member States’ authorities responsible for a FMC. Also, Article 22 of the VTM Directive requires the
Member States to designate the “competent authorities, port authorities and coastal stations” to which
notifications are to be made. A list of such designated authorities is to be shared with the Commission.

\textsuperscript{150} Data controllers are required to take every reasonable step to ensure that data remain accurate and up-
to-date taking into account the purposes for which they were collected of for which they are further
processed (Article 6 (1) (d) of the Data Protection Directive; Article 4 (1) of the Data Protection
Regulation).

\textsuperscript{151} In its interesting Opinion on the principle of availability of law enforcement information (Opinion of
the European Data Protection Supervisor of 28 February 2006 on the Proposal for a Council Framework
Decision on the exchange of information under the principle of availability, \textit{OJ C} 116/8), the EDPS
supports indirect access through the use of “index data” which are defined as “data the purpose of which
is to distinctively identify information and that can be queried by means of a search routine to ascertain
whether or not information is available” (Article 3(g) of the Proposal). According to the EDPS, the
advantage of the use of index data is that it allows the originating Member States to control the exchange
of information from their systems and databases: if consultation of index data results in a match, the
586. Generally, the EDPS stresses that that any interoperability of databases or systems involving personal data must be implemented with due respect for data protection principles and in particular the purpose-limitation principle\(^{152}\).

587. In its Opinion of 28 February 2006 on the exchange of law enforcement information under the principle of availability\(^{153}\), the EDPS underlines that it is essential that the basic principle of purpose-limitation is respected as the various (equivalent) Member State authorities exchanging the data may have a substantially different scope of competences under their national law. According to the EDPS, data collected and processed by a certain authority with a specific purpose cannot then be used for a different purpose just by virtue of the different, possibly broader, competences of the receiving authority. This reasoning can probably also apply to the exchange of maritime data between competent Member State authorities. A precise definition of the **purpose** of the processing (and the purpose of the **sharing** of the data) will therefore be of crucial importance.

588. In fact, in its aforementioned Opinion, the EDPS seems especially concerned with these issues in case of access by law enforcement authorities to data that are held by authorities which are commonly *not* involved in law enforcement (e.g. vehicle registration authorities)\(^{154}\).

589. Therefore, the EDPS considers it essential that the exchange of data because of their availability in a system or database, is subject to a clear definition of: (i) what is meant by “available information”; (ii) who are the (equivalent) designated authorities that will be controlling and exchanging the data; (iii) what are the access conditions for the data; and (iv) what is the purpose of the data exchange between these authorities.

590. Furthermore, the purpose-limitation also has an impact on a number of other issues, such as the time period for the storage or retention of the personal data. Those time limits also have to be seen in the light of the purpose-limitation.

591. Personal data may not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed\(^{155}\).

---

\(^{152}\) See also, for instance, Comments of the EDPS of 10 March 2006 on the Communication of the Commission on interoperability of European databases, available on www.edps.eu.

\(^{153}\) Opinion of the European Data Protection Supervisor of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, OJ C 116/8; the principle of availability entails that information needed for law enforcement purposes should be able to cross the internal borders of the EU without obstacles.


\(^{155}\) Article 6 (1) (e) of the Data Protection Directive; Article 4 (1) (e) of the Data Protection Regulation. For an example in the maritime sector, see Article 37(9) of the Control Regulation which provides that (VMS) data shall only be stored in a form “allowing the identification of the persons concerned” only as long as long necessary for the fulfilment of the purposes in question.
592. Therefore, data accessed or exchanged for one purpose should be deleted as soon it is no longer necessary for that purpose. This should prevent any unnecessary duplication of databases amongst the various authorities who may have access to the data.

593. For the Community institutions and bodies, the purpose-limitation is laid down in Article 4 (1) (b) and (c) of the Data Protection Regulation and further reflected in Articles 6, 7 and 8 of that Regulation.

594. The Data Protection Regulation also contains a specific provision in relation to the “change of purpose”: “personal data shall only be processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body”\(^{156}\).

595. In addition, the Data Protection Regulation also expressly addresses the issue of the sharing of personal data within or between Community institutions and bodies. Article 7 of the Regulation provides that personal data shall only be transferred within or to other Community institutions or bodies “if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient” of the data.

596. It is further provided that where the data are transferred following a request from the recipient, both the data controller and recipient shall bear the responsibility for the legitimacy of the data transfer. In that respect, the data controller is required “to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data”\(^{157}\).

597. Article 7 also explicitly provides that the recipient shall process the personal data “only for the purposes for which they were transmitted”.

598. Article 8 of the Data Protection Regulation addresses the issue of the sharing of personal data by the Community institutions and bodies with recipients which are subject to national data protection laws (e.g. Member States’ authorities or other persons subject to Member States’ data protection laws). Personal data can only be transferred to such recipients:

- (i) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority; or
- (ii) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject’s legitimate interests might be prejudiced.\(^{158}\)

---

\(^{156}\) Article 6(1) of the Data Protection Regulation.

\(^{157}\) The recipient thus needs to establish that the transfer of the data is necessary. If doubts arise as to this necessity, the controller is required to seek further information from the recipient. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified.

\(^{158}\) A Member State authority requesting access to personal data held by a Community institution or body will thus need to establish that the data transfer is necessary, either for the tasks of that public authority or for another reason (provided the data subject’s rights and interests are not prejudiced by the transfer).
The provisions of Article 7 and 8 of the Data Protection Regulation thus clearly demonstrate that the purpose-limitation may affect the ability to share personal data with third party recipients, whether these recipients are Community institutions or not.

A specific reference to the data sharing provision of Article 8 of the Data Protection Regulation can be found in Article 11 of the Register Regulation: Member States are granted access to all of the data contained in the Community register of fishing vessels on condition that they comply with the Data Protection Regulation “and in particular Article 8 thereof” (which means that any personal data from the Community register will only be made available to the Member States if the relevant Member State authority establishes the necessity of the data transfer).

The sharing of data with recipients in non-EEA countries or international organizations

In relation to data sharing, reference should also be made to another important principle (and restriction) of data protection law: the prohibition of the transfer of personal data to recipients outside the European Economic Area (EEA) which do not ensure an adequate level of protection\(^{159}\).

Today, only very few countries are recognised by the European Commission as ensuring such an adequate level of data protection (the “white list” established by the Commission currently remains limited to the following countries: Argentina, Canada, Switzerland, Guernsey, Isle of Man and the United States, provided the US recipient has voluntarily adhered to the Safe Harbour Principles adopted by the US Department of Commerce\(^{160}\).

A transfer of personal data to any country not on the Commission’s white list is in principle prohibited, unless one of the derogations provided for in Article 26 of the Data Protection Directive applies.

According to this Article 26, data export to a country not ensuring an adequate level of protection may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

---

\(^{159}\) Article 25 of the Data Protection Directive; Article 9 of the Data Protection Regulation.

\(^{160}\) Details of the current legal framework in relation to data export outside the EEA are available on: [http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm).
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

605. In addition, data exports to third countries may also be authorised if the data controller has adduced “adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights”\textsuperscript{161}. It is provided that such safeguards may in particular result from appropriate contractual clauses\textsuperscript{162}. For that purpose, the Commission has approved a number of “standard contractual clauses” which EU-based data controllers can use if they intend to transfer personal data to recipients established in third countries not ensuring an adequate level of data protection\textsuperscript{163}.

606. The Data Protection Regulation (applicable to Community institutions and bodies) contains a similar regime (including similar derogations) which not only addresses the export of data to third countries, but also to other “international organisations” (which means no sharing of personal data with international organisations which do not ensure an adequate level of protection)\textsuperscript{164}.

607. Obviously, the restriction on data export to third countries may be particularly relevant for those reporting, surveillance and data sharing mechanisms which would involve a sharing of personal data with the authorities of non-EEA countries or with international organisations\textsuperscript{165}.

6.2.6 Data security

608. Another obvious area of concern in relation to data sharing is the security of the data. Data sharing entails access to a great(er) amount of data by a great(er) number of persons. This can lead to security problems. With the further digitalisation of the economy and society, data security has become one of the most important requirements under data protection law in recent years.

\textsuperscript{161} Reference can be made here to the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement of 23 July 2007). This Agreement enables the sharing of information by European air carriers with the DHS in the US for a limited number of purposes listed in a letter from the US Government to the EU which forms part of the Agreement and which is meant to provide adequate safeguards to the EU with regard to the processing of the PNR data by the relevant US authorities.

\textsuperscript{162} Article 26 (2) of the Data Protection Directive.

\textsuperscript{163} The Commission’s model contracts for the transfer of personal data to third countries can be found on: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

\textsuperscript{164} Article 9 of the Data Protection Regulation; according to paragraph 7 of Article 9, the EDPS may authorize data transfers to third countries or international organizations not ensuring an adequate level of protection if adequate data protection safeguards are put in place (e.g. appropriate contractual clauses).

\textsuperscript{165} For instance, the HELCOM AIS Network seems to involve the sharing of data with Russia (see above, 5.2.1).
609. Controllers of personal data are indeed under a legal obligation to implement appropriate technical and organisational measures to secure the data, i.e. to protect the data against accidental or unlawful destruction or alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing\(^\text{166}\).

610. In particular, the Data Protection Regulation (applicable to Community institutions and bodies) contains detailed provisions with regard to the security of the automated processing of personal data\(^\text{167}\). Also at Member State level, the data security obligation under data protection law may be specified in the law or by means of specific guidelines issued by the local data protection supervisory authorities\(^\text{168}\).

611. In addition, both the Data Protection Directive and the Data Protection Regulation contain a specific provision concerning the “confidentiality” of the processing of personal data\(^\text{169}\). This means that any person employed by the authority that acts as data controller (e.g. Member State authority or Community authority) and having access to personal data is obliged to process the data only on instructions from that data controller (unless he would be otherwise required to do so by national or Community law)\(^\text{170}\).

6.2.7 The rights of the data subjects

612. One other consequence of the applicability of data protection law is that data controllers need to comply with a number of requirements vis-à-vis the data subjects (i.e. the identified or identifiable person to whom the data relate).

613. The rights of the data subject include, inter alia, the right to access and consult the data, the right to request the rectification, erasure or blocking of the data, in particular because of the incomplete or inaccurate nature of the data (or the unlawfulness of the data processing) and a right to object against the data

---

\(^\text{166}\) Article 17 of the Data Protection Directive.

\(^\text{167}\) Article 22 of the Data Protection Regulation, which contains a detailed list of measures to be taken by the Community institutions and bodies to protect the personal data, such as measures to ensure the secure transmission of personal data.

\(^\text{168}\) This is, for instance, the case in Belgium (detailed guidance issued by the Privacy Commission), in Germany (security obligation specified in an Annex to the Data Protection Act), in Finland and the UK (generic guidance issued by the local data protection supervisory authority), and especially in Spain, where Article 17 of the Data Protection Directive was transposed through a very detailed regulation of security measures to be implemented by data controllers (and eventually by data processors), including public bodies. In that respect, it is worth mentioning that (i) among the files that shall be subject to medium level security measures, reference is made to those relating to criminal or administrative offences, while (ii) those containing or referring to data collected by security forces without the consent of the data subjects are subject to high level security measures.

\(^\text{169}\) Article 16 of the Data Protection Directive; Article 21 of the Data Protection Regulation.

\(^\text{170}\) For persons working for public bodies, the observance of confidentiality will usually be part of their official duties, including their general duty of professional secrecy. For instance, Article 10 of the Spanish Data Protection Act provides for a specific duty of professional secrecy with regard to the processing of personal data (applicable also to files controlled by public bodies).
processing under certain conditions (for instance, to object against the use of the data for direct marketing purposes)\(^\text{171}\).

614. In addition, there is an obligation for the data controller to actively inform the data subjects of the data processing. The minimum information to be provided can be found in Articles 10 and 11 of the Data Protection Directive (depending on whether the data were obtained directly from the data subjects or not) and includes *inter alia* information on the identity of the data controller and on the purposes of the data processing. The information needs to be provided except if the data subject already has it.

615. The information obligation of the data controller also includes information on the recipients or categories of recipients of the data “in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject”\(^\text{172}\).

616. Both the Data Protection Directive and the Data Protection Regulation contain a similar derogation from the information obligation where the data would not have been directly obtained from the data subject (but, for instance, would have been acquired from a third party database)\(^\text{173}\). In that case, the data controller does not need to provide the information if this proves impossible\(^\text{174}\) or involves a disproportionate effort\(^\text{175}\), or if recording or disclosure of the data would be expressly laid down by law. In these circumstances, Member States (or Community institutions or bodies) are nevertheless required to provide appropriate safeguards.

617. With regard to the specific information obligation under data protection law, reference can be made to the letter which the UK DEFRA addressed to the owners of registered fishing vessels and fishing vessel license entitlement holders on 10 May 2002. This letter was clearly sent by DEFRA to comply with the information requirements imposed by the UK Data Protection Act of 1998 (which implements the Data Protection Directive into UK law).

To the owners of registered fishing vessels and fishing vessel licence entitlement holders in England and Wales

10 May 2002

FISHERIES: DATA PROTECTION ACT 1998

\(^{171}\) See Articles 12 to 15 of the Data Protection Directive or the entire Section 5 of the Data Protection Regulation.

\(^{172}\) Articles 10 and 11 of the Data Protection Directive; for Community institutions and bodies, the obligation to provide information on “the recipients or categories of recipients” of the data is slightly stronger as it is not linked to the condition that this information needs to be necessary to guarantee a fair processing towards the data subject (cf. Articles 11 and 12 of the Data Protection Regulation). The scope of the information obligation for Community institutions and bodies is also broader than the obligations laid down by the Data Protection Directive (and includes *inter alia* information on the legal basis of the processing, the time-limits for storing the data and the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy).

\(^{173}\) Article 11 (2) of the Data Protection Directive; Article 12 (2) of the Data Protection Regulation. In both Articles, the derogation is provided “in particular for processing for statistical purposes or for the purposes of historical or scientific research”.

\(^{174}\) For instance, because the data controller does not have the contact details of the data subjects.

\(^{175}\) For instance, because a very large number of data subjects is involved.
As you will be aware, as part of our obligations for the management and control of the Common Fisheries Policy, DEFRA collects and holds a range of information and data on the fishing industry and related activities. This is covered by the provisions of the Data Protection Act and the purpose of this letter is to advise you, in accordance with that Act, of how we shall use and process the data.

You will wish to note that information collected and held by DEFRA on the catching, landing, marketing and transport of fish and fisheries products, fishing vessel activity, fishing vessel sightings, satellite position reports and fishing vessel licences will be used by DEFRA for the purposes of the management, monitoring and control of the Common Fisheries Policy and for other conservation, management, control and enforcement functions. In order to perform these functions, such data may be disclosed to DEFRA’s agencies and authorised agents, the other Fisheries Departments in the UK, other government departments, relevant authorities in the European Commission, other Member States and third countries. Satellite position reports and other sightings data will also be made available, on request, to the UK Coastguard for search and rescue purposes.

DEFRA may also publish or disclose such data, in an anonymous and/or aggregated form, to other organisations, bodies or persons for other purposes, including scientific research.

If you require any clarification on the issues raised in this letter you are advised to contact (Mrs A. Person), Room 1234 at the above address (Tel: 020 123 4567; Fax 020 123 4568; Email: A.Person@defra.gsi.gov.uk).

A copy of this letter is also being sent to the NFFO and to POs in England and Wales for information.

618. DEFRA is thus clearly of the opinion that the data it collects and processes for the management, monitoring and control of the CFP includes personal data and that, as a consequence, it needs to comply with local data protection laws and regulations, including the specific information obligation imposed upon data controllers.

619. With regard to the right of access and rectification of the data subjects and the information obligation of the data controllers, it should be noted that both the Data Protection Directive and the Data Protection Regulation provide for a possibility to restrict the scope of these provisions.

620. In accordance with Article 13 of the Data Protection Directive, the Member States are allowed to implement such restrictions (by legislative means) if this is necessary to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the EU (including monetary, budgetary and taxation matters);
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in the cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

621. Article 20 of the Data Protection Regulation contains a largely similar provision applicable to Community institutions and bodies.

176 The acronym NFFO stand National Federation of Fishermens’ Organisations, while POs stands for Producer Organisations.
Box G – Restriction of the scope of Member State data protection laws

Member States have used the possibility granted by Article 13 of the Data Protection Directive to restrict the scope of their national data protection laws in certain circumstances, especially in relation to public security and law enforcement matters.

- For instance, in **Germany**, Section 14 §2 of the Data Protection Act provides that, under certain, specified conditions, the storage, modification or use of personal data by public authorities is admissible, even if it is not required for the performance of the duties of the controller and for the purposes for which the data were initially collected. Such conditions are, in particular: if “a legal provision prescribes or peremptorily presupposes this”, or if it is necessary “in order to avert substantial detriment to the common weal or a threat to public security, or to protect substantial interests of the common weal”, or “to prosecute criminal or administrative offences, to implement sentences or measures” (*inter alia* in the sense of the Criminal Code), or “to avert a grave infringement of another person’s rights”. However, even if the above-mentioned conditions are fulfilled, a transfer of personal data to other public bodies is only admissible if it is necessary for the performance of the duties of the sender or receiver of the data.

- In **France**, the Data Protection Act provides for limitations to the information of data subjects and to their right of access in case of processing operations carried out by public authorities, notably where the processing is related to State security or the prosecution of offences.

- In **Spain**, Article 13 of the Data Protection Directive was implemented by Articles 22 to 24 of the Data Protection Act providing i.a. that the collection and processing of personal data by the security forces without the consent of the data subjects shall be limited to those cases and categories of data necessary for the prevention of a genuine threat to public safety or for the suppression of crime (and that such data shall be stored in special files which must be classified according to their degree of reliability).

- In **Finland**, Section 24 of the Data Protection Act provides that the duty of providing information (on the controller and on the purpose of the processing, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question) may be derogated from if this is necessary for *inter alia* the protection of national security, defence or public order or security, or for the prevention or investigation of crime.

- In the **UK** also, there are significant exemptions in relation to national security and crime prevention and detection. For instance, with regard to national security, data controllers may be exempted from the obligation to comply with the data protection principles and the rights of data subjects. In addition, the Information Commissioner’s Office will not have a right to bring enforcement action if this exemption is relied upon, and it will not be an offence to unlawfully obtain personal data. In order to rely on this exemption, certain ministers of the Crown are required to certify that an exemption is required. The certification will be considered to be conclusive (although there is a right of appeal for anyone who is directly affected by the issuing of the certificate).  

### 6.2.8 Legitimacy of the processing of personal data within the framework of maritime reporting and surveillance

622. Article 7 of the Data Protection Directive sets out the criteria for making data processing legitimate. Member States are required to provide that personal data may be processed only if certain conditions are met. These conditions include *inter alia* “if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed” (emphasis added)\(^\text{177}\). It is of course this condition that, in most cases, will form the legal basis for the processing (including the sharing) of personal data within the framework of maritime reporting and surveillance at Member State level.

---

\(^{177}\) Article 7(e) of the Data Protection Directive; a data controller performing a task carried out in the public interest or in the exercise of official authority can either be a public administration or another natural or legal person governed by public law, or by private law (such as a professional association). The Member States are free to determine this (cf. recital (32) of the Data Protection Directive).
623. Similarly, the Data Protection Regulation (Article 5) contains an equivalent provision allowing the processing of personal data if “processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed …” (emphasis added).

624. Examples of other criteria which can make a processing of personal data legitimate include: (i) the unambiguous consent of the data subject; (ii) the necessity for the data controller to comply with a legal obligation; (iii) the necessity for the performance of a contract with the data subject; (iv) the necessity to protect the vital interests of the data subject; and (v) the legitimate interests of the data controller (or the third party recipient of the data) except where such interests would be overridden by fundamental rights and freedoms of the data subject e.g. the right to privacy.

625. Except for the latter one (legitimate interests of the data controller), these criteria are also provided for in the Data Protection Regulation (Article 5).

6.2.9 Activities falling outside the scope of data protection law

626. Finally, it is important to note that not all processing of personal data automatically falls under the scope of the existing data protection legislation (i.e. Data Protection Regulation, Data Protection Directive and implementing laws at Member State level). There are a number of exceptions which are explicitly provided for in the Data Protection Directive and Data Protection Regulation. Some of these exceptions may be of relevance for this Study.

627. According to its Article 3(2), the Data Protection Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law (i.e. second and third pillar activities such as the common foreign and security policy and the police and judicial cooperation in criminal matters)\(^{178}\). The CFP and maritime transport obviously fall within the scope of Community law and are therefore in principle subject to the existing data protection legal framework (if personal data are processed for purposes which fall within that scope).

628. Article 3(2) of the Data Protection Directive further specifies that its provisions shall “in any case” not apply to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing relates to State security matters) and the activities of the State in areas of criminal law. The processing of maritime data for military purposes, as well as for State security and (criminal) law enforcement purposes is thus currently in principle exempted from the scope of the existing data protection legal framework (in so far as such maritime data would contain personal data). The same applies to the processing of personal data in the framework of police and judicial co-operation.

\(^{178}\) Similarly, Article 3 (1) of the Data Protection Regulation provides that the Regulation applies to the processing of personal data by all Community institutions and bodies “insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law”.

123
between the Member States in criminal matters. The protection of personal data may nevertheless be addressed in various specific instruments in this field and may thus have to be complied with on an ad hoc basis\textsuperscript{179}.

### Box H – Data protection law exclusions

Member States will typically exclude from the scope of their national data protection laws any processing of personal data by their national security and intelligence services (including the military services) and by their judicial and other police forces (including the supervisory authorities of these forces). On the other hand, certain types of processing may be subject to specific data protection provisions contained in other laws (in addition to the applicability of the generic data protection law),

- For instance, in **Spain**, data files subject to rules on classified information, as well as data files created for the investigation of terrorism and other organised serious crime, are exempted from the applicability of data protection law. However, in these cases, the controller of the data file remains obliged to previously communicate its existence, its features and its purpose to the Spanish Data Protection Agency. On the other hand, it is provided in the Data Protection Act that certain types of personal data files shall be governed both by (i) the Data Protection Act and (ii) by specific legal provisions, such as those applicable to images and sound recorded by the video cameras of the security forces\textsuperscript{180}. The Spanish Data Protection Act (Article 21) also contains special rules in relation to the disclosure of data between public authorities (in substitution of the general rules applicable to communications of data, which are based on the principle of consent of the data subject). For instance, it is provided that “personal data collected or drawn up by public administrations in the performance of their tasks shall not be communicated to other public administrations for the exercise of different powers or powers relating to other matters unless the communication is for the purpose of subsequent processing for historical, statistical or scientific purposes”.

- In **Malta**, rules on the collection, processing and communication of personal data by public bodies exercising police powers is dealt with in specific regulations (Processing of Personal Data in the Police Sector Regulations of 2004).

- In the **UK**, the Data Protection Act contains a list of exemptions, including *inter alia* national security and crime prevention and detection.

- Also in **France**, specific rules are provided with regard to the processing of personal data by public sector authorities, notably if the processing involves State security, defence or public safety, or the prevention, investigation, or proof of criminal offences, the prosecution of offenders or the execution of criminal sentences or security measures.

- In **Finland**, the Data Protection Act is considered as a generic Act in relation to the processing of personal data; the provisions of the Act apply, unless otherwise provided elsewhere in the law. Therefore, should any specific Act contain rules regarding processing of personal data, such Act shall prevail over the Data Protection Act. In this respect, there is specific legislation concerning the processing of personal data e.g. within the public sector (the Act on the Openness of Government Activities 621/1999, as amended), by the police (the Act on the Processing of Personal Data by the Police 761/2003) and by Border Guard Service (the Act on Processing of Personal Data by the Border Guard Service 579/2005). For instance, the Act on the Processing of Personal Data by the Police specifies what kind of personal data the police is entitled to collect, process and disclose.

- Also in **Germany**, the Data Protection Act contains rules on precedence regarding other laws that concern or include the use of personal data. It is provided that other Federal legal provisions shall take precedence over the provisions of the Data Protection Act in so far as they are applicable to personal data, including their publication. An example of such an area-specific law is the Maritime Matters Act (see above). The collection, processing and use of personal data by the public bodies of the Länder is generally governed by the local Data Protection Acts of the respective Länder.

629. It is, however, important to stress that, in addition to the Data Protection Directive and the Data Protection Regulation, a Commission Proposal for a Council

\textsuperscript{179} For instance, Article 23 of the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197 of 12 July 2000. The EUROPOL Convention also addresses the protection of personal data (cf. Articles 14 – 25), including provisions on the use of data, data security and the communication of data to third States and third bodies.

\textsuperscript{180} Organic Act 4/1997 on Use of Video Cameras by the Public Security Bodies and Forces in Public Places and its secondary regulations.
Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters is currently being discussed.\(^{181}\)

630. The proposed Framework Decision should ensure the protection of personal data within the framework of the EU’s third pillar. This particularly concerns the sharing of data between Member States for the purpose of preventing and combating crime. In that respect, Article 8 of the draft Proposal specifically addresses the issue of the transmission of and making available of personal data to the competent authorities of other Member States: “Member States shall provide that personal data shall only be transmitted or made available to the competent authorities of other Member States if necessary for the fulfillment of a legitimate task of the transmitting or receiving authority and for the purpose of the prevention, investigation, detection or prosecution of criminal offences” (emphasis added).

631. Section 2 of the Proposal contains detailed conditions for the further processing of the data, in particular the further transmission and transfer of the shared data to other competent authorities, to other than competent authorities, to private parties and to authorities in third countries or to international bodies.

632. Obviously, this proposal is closely linked to the Commission’s Proposal for a Council Framework Decision on the exchange of information under the principle of availability.\(^{182}\) This Proposal aims at determining the conditions and modalities for the exchange of certain information between “equivalent competent authorities”\(^{183}\) for the (exclusive) purpose of assisting these authorities in their tasks of preventing, detecting and investigating criminal offences.

633. The information that may be exchanged under this proposed Framework Decision is listed in Annex II of the Proposal and obviously includes personal data such as DNA-profiles, fingerprints, telephone numbers, but also vehicle registration data and data for the identification of persons “contained in civil registers”.

634. In relation to the exchange of personal data, questions may arise as to the sharing of data between (third pillar) law enforcement authorities on the one hand and (first pillar) authorities not involved in law enforcement on the other hand. The EDPS has already expressed concerns about the potential legal loophole that this may create, \(i.e.\) which legal regime will apply to the processing: the first pillar or the (future) third pillar regime? This issue may be relevant for this Study to the extent that it would be envisaged to share any routinely collected maritime reporting and surveillance data (e.g. VMS data) with authorities which are specifically involved in the enforcement of criminal law (e.g. police or judicial authorities).

---


\(^{183}\) Article 5 and Annex III of the Proposal (COM/2005/490final) contain the criteria to determine the equivalence of competent authorities.
635. In this respect, reference can also be made to the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes\(^{184}\), which provides for the making available by air carriers of PNR data to “the competent authorities of the Member States”\(^{185}\) for the purpose of “preventing and combating terrorist offences and organised crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them” (emphasis added). The Proposal foresees the designation in each Member State of a specific unit (Passenger Information Unit) responsible for the collection of the PNR data and for carrying out a risk assessment of passengers. Information assessed accordingly will be transmitted to competent authorities in the other Member States on a case-by-case basis and only for the purpose indicated above\(^{186}\).

636. It can be assumed that similar legal safeguards may need to be put in place for the sharing of any routinely collected maritime reporting or surveillance data (i.e. personal data) by competent authorities (e.g. VMS data collected by FMCs for the purpose of the monitoring of fishing vessels) with law enforcement authorities for the specific purpose of the prevention, investigation, detection or prosecution of criminal offences.

### 6.3 Data (security) policies of public authorities

637. Another barrier to data exchange may potentially be found in the rules with regard to the classification of data (data policy) of the relevant European institutions and bodies and equivalent rules and policies at Member State level. These rules are usually adopted to develop and safeguard activities in areas which require a certain degree of confidentiality.

638. For instance, the sharing of confidential information or data within the Commission or between the Commission and Member States is regulated in the Commission Decision of 29 November 2001 amending its internal Rules of Procedure\(^{187}\). By this Decision, the Commission adds its “rules on security” to its Rules of Procedure. In Section 4.2 of the Rules on Security, the broad concepts of “EU classified information” (EUCI) and “document” are further defined and clarified.

639. The term “document” is broadly defined as “any letter, note, minute, report, memorandum, signal/message, sketch, photograph, slide, film, map, chart, plan, notebook, stencil, carbon, typewriter or printer ribbon, tape, cassette, computer disk, CD-ROM, or other physical medium on which information has been recorded”.

---


\(^{185}\) These “competent authorities” must only be authorities responsible for the prevention or combating of terrorist offences and organised crime. Member States are required to draw up a list of such authorities and to share it with the Commission.

\(^{186}\) The EDPS has already expressed serious concerns with regard to the legitimacy, proportionality and necessity of the proposed measures (Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, \(OJ\ C-110/1\) of 5 January 2008). The EDPS calls \textit{inter alia} for a more precise description of the potential recipients of the data and their respective competences.

\(^{187}\) \(OJ\ L 317/1\) of 3 December 2001.
Maritime reporting or surveillance data (signals, messages, pictures, etc.) could thus fall within the scope of this data security policy. It is however nowhere mentioned whether there is any distinction to be made between information that is originating from or generated by the Commission itself, on the one hand, and information that is received by the Commission from a Member State, on the other hand.

The term “EU classified information” is defined as “any information and material, an unauthorized disclosure of which could cause varying degrees of prejudice to EU interests, or to one or more of its Member States, whether such information originates within the EU or is received from Member States, third States or international organizations”.

The Commission imposes four levels of classification of information (Section 16 of the Decision), whereby no other (external) classifications are permitted, namely:

(a) “EU TOP SECRET”: this classification is applied only to information and material the unauthorized disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of its Member States;
(b) “EU SECRET”: this classification is applied only to information and material the unauthorized disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States;
(c) “EU CONFIDENTIAL”: this classification is applied to information and material the unauthorized disclosure of which could harm the essential interests of the European Union or of one or more of its Member States;
(d) “EU RESTRICTED”: this classification is applied to information and material the unauthorized disclosure of which could be disadvantageous to the interests of the European Union or of one or more of its Member States.

The personal scope of application of this data sharing policy is also rather wide since the rules with regard to handling EU classified information need to be respected not only within the Commission itself, but also by every institution/person liaising with the Commission.

It is stipulated that the rules of security need to be respected by Commission officials and other servants, by personnel seconded to the Commission, as well as within all Commission premises, including its Representations and Offices in the Union and its Delegations in third countries and by contractors external to the Commission.

It is further provided that Member States, other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties shall be allowed to receive EU classified information on the condition that they ensure that, when EU classified information is handled, rules strictly equivalent to the Commission’s rules on security are respected within their services and premises, in particular by:

188 Article 2 of the Commission Decision.
(a) members of Member States’ permanent representations to the European Union as well as by members of national delegations attending meetings of the Commission or of its bodies, or participating in other Commission activities;
(b) other members of the Member States’ national administrations handling EU classified information, whether they serve in the territory of the Member States or abroad;
(c) external contractors and seconded personnel, handling EU classified information.

Box I – Member State data security policies

Equivalent data security policies may of course exist at Member State level and will have to be complied with by the relevant authorities and bodies.

- In Germany, public authorities may be bound by different internal data security policies. Depending on the employing public authority, the legal basis varies. The scope of the different policies is comparable. For instance, the Rules on Document Security (Geheimschutzordnung) of the Bundestag (German Parliament), provide for the following security classifications:
  - TOP SECRET (streng geheim, str. geh.)
  - SECRET (geheim, geh.)
  - CONFIDENTIAL (Verschlusssache-vertraulich, VS-Vertr.)
  - RESTRICTED (Verschlusssache- Nur für den Dienstgebrauch, VS-NfD.)
  
  Classified material is defined as material regarding matters of any kind in whatever form that must be prevented by means of special security measures from coming to knowledge of unauthorized persons. The same classification is provided for in the Rules on Document Security of other public authorities, such as the Bundesrat (Federal Council). Further, administrative personnel of the different (Federal) Ministries and Länder authorities are bound by corresponding administrative regulations on data security. In general, the rank and scope of official duties of a civil servant or employee of public authorities determine the access rights to classified material. Access to the classification "CONFIDENTIAL" and higher requires a specific authorisation following a formalised procedure.

- In France, Decree n°98-608 of 17 July 1998 with respect to the protection of national defence secrets provides for three different levels of confidential information:
  - Très-Secret-Défense” applies to information or protected media whose disclosure is likely to harm very seriously the national defence and which are related to the priorities of the government in the field of defence;
  - “Secret-Défense” applies to information or protected media whose divulgation is likely to harm seriously the national defence;
  - “Confidentiel-Défense” applies to information or protected media whose disclosure is likely to harm the national defence or could lead to the disclosure of information defined as defence secret or high defence secret.

- In Finland, public authorities are also bound by internal data security policies; however, these policies are usually not publicly available.

- Also in Malta, this type of policies would rather be unavailable to the public and may vary from one authority to another, depending on the importance and nature of the data and the gravity of the consequences if the data is divulged.

- In Spain, the potential classification of information (as “secret” or “restricted”) by the public administration is mainly regulated in Act 9/1968 on Official Secrets which sets forth the requirements, procedures and consequences for such classification to be decided by the government.

646. Data security policies, such as the one of the Commission referred to above, may imply different degrees of information security and could therefore constitute a possible barrier to the free dissemination and sharing of maritime surveillance and monitoring data between Member States, in so far the information would also circulate through the Commission and would be marked as EU classified information. That would trigger the need for those handling the data to comply with the foregoing policy rules.
Data security and classification policies may especially be relevant for the military authorities who, obviously, will not share any of their maritime surveillance data if the data is considered classified under their (internal) data security rules. The classification of certain military surveillance data may be linked to the way the data were collected (e.g. the use of certain tools or technologies which are secret) or the fact that routinely collected maritime data were combined with specific military intelligence data.

A specific example of classification of maritime surveillance data can be found in the (military) sea-surveillance co-operation between Finland and Sweden (SUCFIS, see above 5.5). Section six of the Agreement between the Ministry of Defence of Finland and the Swedish Armed Forces concerning Sea Surveillance Co-operation imposes the following three levels of security classification of maritime surveillance data:

**IN FINLAND**                  **IN SWEDEN**

SALAINEN                        HEMLIG / SECRET

LUOTTAMUKSELLINEN               HEMLIG / CONFIDENTIAL

VIRANOMAISKÄYTTÖ               HEMLIG / RESTRICTED

The Agreement also contains further rules with regard to the access to the classified surveillance data, the sharing of the data with governmental authorities, the transmission of the data (and the security of such transmissions, including a security breach notification scheme).

### 6.4 Re-use of public sector information

In relation to potential obstacles to data sharing, reference could also be made to Directive 2003/98/EC on the re-use of public sector information of 17 November 2003 (hereinafter the “PSI Directive”) which provides for minimum rules applicable in all the Member States as to the re-use of public sector information resources.

The aim of the PSI Directive is to lower the barriers which individuals or companies face while they develop new cross-border information services and products. The PSI Directive had to be implemented by all EU Member States by 1 July 2005.

Re-use of public sector information is generally defined as “the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced”\(^{189}\).

The PSI Directive does not require Member States to allow the re-use of public sector information, but states that “where re-use of documents held by public authorities is allowed”, these documents need to be re-usable for commercial and non-commercial purposes in accordance with the conditions laid down in the

---

189 Article 2, (4) of the PSI Directive; “documents” is broadly defined by the PSI Directive as “any content whatever its medium” (and any part of such content).
Directive (and where possible, the documents should then be made available through electronic means)\textsuperscript{190}.

654. As a general rule the PSI Directive does not apply to, \textit{inter alia}, the following categories of data/documents\textsuperscript{191}:

(a) documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or in the absence of such rules as defined in line with common administrative practice in the Member State in question;
(b) documents for which third parties hold intellectual property rights;
(c) documents which are excluded from access by virtue of the access regimes in the Member States, including on the grounds of (i) the protection of national security (\textit{i.e.} State security), defence, or public security, or (ii) statistical or commercial confidentiality\textsuperscript{192}.

655. Particularly with regard to point (c) above, whether maritime surveillance and reporting data could fall under any of the exempted categories of data/documents may depend on the circumstances of the case and the guidelines and practices in relation to data access adopted throughout the various Member States.

656. However, on this basis, it cannot be excluded that maritime surveillance and reporting data would be exempted from the scope of the PSI Directive, for instance in so far as certain of these data may be legally qualified as (commercially) confidential. In that case, Member States could decide, even if they generally allow re-use of public sector data, that these specific data are not to be made available under the PSI regime.

657. Further, it is important to note that the PSI Directive is, in principle, not applicable to the sharing of documents “between public sector bodies purely in pursuit of their public tasks”\textsuperscript{193}. Such exchange of documents is not considered to be “re-use”\textsuperscript{194} and is thus not affected by the provisions of the PSI Directive.

658. Although this is nowhere explicitly stated, it can be understood that not only the exchange of data between public authorities in the same Member State, but also the cross-border sharing of data between various Member States is considered to be exempted.

659. However, the PSI Directive does not, as such, exclude the situation where public sector bodies (trans)act themselves in the private or commercial sphere (\textit{e.g.} resale of data to commercial companies); this situation will then fall under the regime of the PSI Directive.

\textsuperscript{190} Article 3 of the PSI Directive.
\textsuperscript{191} Article 1 (2) of the PSI Directive.
\textsuperscript{192} With regard to access regimes, see below, 6.5.
\textsuperscript{193} “Public sector body” is defined as “the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law” (Article 2 of the PSI Directive, which also further defines the concept of “body governed by public law”).
\textsuperscript{194} Article 2, (4) of the PSI Directive.
The legal regime on re-use of public sector information may also be an issue if certain Member State surveillance or monitoring bodies, involved in the maritime data sharing, would be operating under a (semi)privatized structure (e.g. under a public private partnership or with operations outsourced to a private operator). In such circumstances, the legal regime of the PSI Directive could apply and may possibly affect the transfer of data by public sector bodies in Member States towards such non-public operators. For instance, public sector bodies in Member States would then in principle be allowed, under the PSI regime, to impose licence conditions (and charges) to non-public sector operators requesting access to the data for re-use. They could then also decide to withhold access to certain data on one of the grounds set out in Article 1 (2) of the PSI Directive (for instance, because the data are protected by confidentiality or in the interest of national security, see above).

6.5 Access to public sector documents (freedom of information)

In addition to the specific data (security) policies of public authorities and the (potential) issues related to Member States’ implementation of the re-use of PSI Directive regime, potential restrictions to data access may also be found in the “public access” (or “freedom of information”) laws and regulations which exist at both EU and Member State level and which usually contain a number of grounds for refusal of access to certain data.

6.5.1 Public access to Community documents

The main legal instrument at EU level is Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (hereinafter the “Transparency Regulation”). The purpose of this Regulation is to give effect to the right of public access to documents and to lay down the general principles and limits on such access in accordance with Article 255(2) of the EC Treaty. The Community system of access to documents is similar to systems of access in force in most Member States that have legislation in this field.

The Transparency Regulation applies not only to documents drawn up by the institutions but also to documents received by them, in all areas of activity of the EU. In principle, all documents of the institutions should be accessible to the public. The purpose of the Transparency Regulation is to ensure the widest and easiest possible access to documents. However, the Transparency Regulation

---

195 For instance, privatised port authorities.
196 Article 8 of the PSI Directive.
197 OJ L 145/43.
198 Article 255 (1) of the EC Treaty provides a general right of access to European Parliament, Council and Commission documents for “any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State”.
199 Article 2 (3) of the Regulation; second and third pillar documents are thus falling within the scope of the Regulation (contrary to the Data Protection Regulation, see above, 597).
200 “Document” is defined by Article 3(a) of the Regulation as “any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a matter relating to the policies, activities and decisions falling within the institution’s sphere of
recognizes that certain public and private interests may need to be protected by way of exception to the general rule. Therefore, the Transparency Regulation lays down a number of exceptions where the institutions may refuse access. In the same way, the Transparency Regulation provides for a special treatment of documents with a highly sensitive content.

664. The beneficiaries of the access right provided under the Transparency Regulation are the citizens of the EU and all natural or legal persons residing or having their registered office in a Member State. Institutions may also grant access to natural or legal persons not residing or not having their registered office in a Member State, subject to the same principles, conditions and limits.

665. The Transparency Regulation is without prejudice to any existing rights of access to documents for Member States, judicial authorities or investigative bodies. The Regulation is also without prejudice to any rights of public access that would be granted by instruments of international law or by acts of the institutions implementing those instruments.

666. The exceptions to the general rule of accessibility are laid down in Article 4 of the Transparency Regulation.

667. Article 4 (1) of the Transparency Regulation allows the institutions to refuse access to a document “where disclosure of that document would undermine the protection of:

a) the public interest as regards:
   - public security,
   - defence and military matters,
   - international relations,
   - the financial, monetary or economic policy of the community or a Member State;

b) privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.

668. These exceptions are compulsory and absolute: should disclosure of a document cause harm to one of the interests mentioned, then access must be refused.

669. In accordance with Article 4(2), the institutions must also refuse access to a document where disclosure of that document would undermine the protection of:

   - the commercial interests of a natural or legal person, including intellectual property.

201 Article 9 of the Regulation; it is also provided in the Regulation that each institution should respect its own (data) security rules and that Member States should respect these rules (see also above, 6.3).

202 In addition, Article 16 of the Regulation provides that the Regulation is without prejudice to any existing rules on copyright which may limit a third party’s right to reproduce or exploit released documents.

203 The purpose of this exception clearly is to protect the business secrets and interests (including reputation) of undertakings which they may have communicated in the context of investigations relating...
court proceedings and legal advice,
- the purpose of inspections, investigations and audits.\textsuperscript{204}

670. These exceptions are compulsory but not absolute: they apply unless there is “an overriding public interest in disclosure”. This means that the information will have to be made accessible if the balance of interests shows an overriding public interest in disclosure (even if the information could reasonably fall under one of the exceptions).

671. In the same way, access to documents drawn up by an institution for internal use or received by an institution, and which relate to a matter where the decision has not (yet) been taken by the institution, shall be refused if disclosure of the document would seriously undermine the institution’s decision-making process (again, unless there would be an overriding public interest in disclosure).\textsuperscript{205}

672. As regards third party documents (for instance, documents of Member State authorities or of private undertakings), the institution must consult the relevant third party with a view to assessing whether one of the exceptions in Article 4(1) or (2) could apply (unless it is clear that the document shall or shall not be disclosed).\textsuperscript{206}

673. Also, Member States may request an institution not to disclose a document originating from that Member State without its prior agreement.\textsuperscript{207} On the other hand, if Member States receive a request for access to a document in their possession, originating from an institution, they must consult with that institution in order to take a decision that remains in line with the objectives of the Transparency Regulation (unless it is clear that the document shall or shall not be disclosed).\textsuperscript{208}

674. In addition to the exceptions that the institutions could invoke in order to refuse access to certain information, Article 9 of the Transparency Regulation also contains a specific provision with regard the treatment of “sensitive documents”.

675. Sensitive documents are documents originating from the institutions or their agencies, from Member States, third countries or international organisations, which


\textsuperscript{205} Article 4(3) of the Regulation.

\textsuperscript{206} Article 4(4) of the Regulation.

\textsuperscript{207} Article 4(5) of the Regulation.

\textsuperscript{208} Article 5 of the Regulation.
are classified as “TOP SECRET”, “SECRET” or “CONFIDENTIAL” in accordance with the data security rules and policies of the relevant institution and which protect essential interests of the EU or of one or more of its Member States in the areas covered by Article 4(1)(a) of the Transparency Regulation (notably public security, defence and military matters). Sensitive documents may be released only with the consent of the originator.

676. An institution which decides to refuse access to a sensitive document must give the reasons for its decision in a manner which does not harm the interests protected in Article 4 of the Transparency Regulation. Institutions are also required to make their rules concerning sensitive documents public.

677. Obviously, if certain maritime reporting and surveillance data would qualify as sensitive information within the meaning of the Transparency Regulation, this might constitute a barrier to the free movement of these data between the institution holding the data and any other interested third party (see also above, 6.3).

678. Otherwise, the exceptions to the general principle of accessibility are to be interpreted in a restrictive way. For instance, if only parts of the requested document are covered by any of the exceptions set out in Article 4 of the Transparency Regulation, then the remaining parts of the document must be released.

679. It is also provided that the exceptions only apply for the period during which protection is justified on the basis of the content of the document and not longer than a period of 30 years. However, in the case of documents covered by the exceptions relating to privacy or commercial interests and in the case of sensitive documents, the exceptions may, if necessary, continue to apply after 30 years.

680. The European Community case law based on the Transparency Regulation also shows that the exceptions to the right of access need to be interpreted in a (very) restrictive way. Often, applicants have pleaded that institutions applied or interpreted the exceptions of Article 4 of the Transparency Regulation in an incorrect way and brought their case before the European Courts.

681. Particularly interesting, in that respect, is the Bavarian Lager case where the Court of First Instance was called to examine the interaction between the “privacy/data protection” exception provided for in Article 4(1)(b) of the Transparency Regulation and the Data Protection Regulation (applicable to Community institutions and bodies).

---

209 In relation to data security policies, see above, 6.3.
210 Sensitive, classified documents are thus as such not excluded from the right of access.
211 Article 4(7) of the Regulation.
212 By way of example: judgement of the Court of First Instance of 13 April 2005, Verein für Konsumenteninformation, Case T-2/03: ‘exceptions to the principle of access to documents must be interpreted strictly’.
213 Judgment of the Court of First Instance of 8 November 2007, The Bavarian Lager Co. Ltd., Case T-194/04, currently under appeal before the Court of Justice.
214 In this case, the Commission refused to disclose the names of the persons who had attended a meeting. The Commission held that it had to apply the Data Protection Regulation and that the applicant had not demonstrated the necessity of the data transfer, as required by Article 8 of the Data Protection Regulation (see also above).
In this case, where the applicant was actually supported by the EDPS, the Court basically held that the right of access provided under the Transparency Regulation overrides the principles of data protection laid down by the Data Protection Regulation: “where personal data are transferred in order to give effect to Article 2 of the Transparency Regulation, laying down the right of access to documents for all citizens of the Union, the situation falls within the application of that Regulation and, therefore, the applicant does not need to prove the necessity of disclosure for the purposes of Article 8(b) of Regulation 45/2001”. The Commission could therefore not validly refer to the requirements of the Data Protection Regulation to refuse the sharing of personal data with a party requesting access to those data in accordance with the Transparency Regulation.

The exception to Article 4(1)(b) of the Transparency Regulation, which allows to refuse access to information in the interest of “privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data”, is interpreted by the Court in a very strict way which basically limits the scope of the exception to the mere protection of the private life of individuals as well as the integrity of their person215.

In this respect, it can be assumed that in relation to maritime reporting and surveillance, the majority of the personal data involved will be business-related and therefore not of a nature to affect the private life or personal integrity of the individuals concerned (e.g. vessel owners)216.

Finally, in relation to public access to Community documents, it should be noted that very recently, on 30 April 2008, the Commission issued a Proposal for a (new) Transparency Regulation217.

One of the reasons for the review of the existing Transparency Regulation is precisely the case law that was developed on the basis of this Regulation. For instance, it is proposed to clarify and amend the “privacy/data protection” exception of Article 4(1)(b) taking into account the restrictive findings of the Court of First Instance in the aforementioned Bavarian Lager case.

6.5.2 Public access to environmental information


The objective of the Environmental Information Directive is to guarantee the right of access to environmental information held by, or for, public authorities and

---

215 The Court found that the fact that the minutes of a meeting contain the names of the participants to that meeting does not affect the private life of these persons given that they participated in the meeting as representatives of the (professional) bodies to which they belonged.

216 It would probably be different if the data would concern pleasure boats or yachts, or for instance passenger lists.


to set out the basic terms and conditions of, and practical arrangements for, the exercise of this right of access\textsuperscript{219}.

689. The Environmental Information Directive is of interest as certain data processed within the framework of maritime surveillance and reporting schemes could be classified as “environmental information” within the meaning of this Directive.

690. This may, for instance, be the case where “environmental information” is defined as including “any information in written, visual, aural, electronic or any other material form on: (...) factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment”(emphasis added), or where the definition concerns “activities affecting or likely to affect” the elements and factors of the environment\textsuperscript{220}.

691. In particular, certain Hazmat and VMS data may fall within these definitions and may therefore be affected by the provisions of the Environmental Information Directive.

692. Applicability of the Environmental Information Directive means that Member States must ensure that their public authorities are required to make available environmental information held by or for them to any applicant requesting for that information\textsuperscript{221}.

693. This also means that Member States may provide for a request for environmental information to be refused if one of the exceptions laid down by Article 4 of the Environmental Information Directive can be applied.

694. This includes the refusal of access because the disclosure of the information would adversely affect:

a) the confidentiality of the proceedings of public authorities, where such confidentiality is provided for by law;
b) international relations, public security or national defence;
c) the course of justice, the ability of any person to receive a fair trial or the ability of a public authority to conduct an enquire of a criminal or disciplinary nature;
d) the confidentiality of commercial or industrial information where such confidentiality is provided for by national or Community law to protect a legitimate economic interest\textsuperscript{222}, including the public interest in maintaining statistical confidentiality and tax secrecy;
e) intellectual property rights;

\textsuperscript{219} Member States had to implement the Environmental Information Directive by 14 February 2005. As with any Directive (for instance the Data Protection Directive or the PSI Directive), local variations may exist in the implementation measures of the Environmental Information Directive throughout the Member States (although not with regard to the general principles laid down by the Directive).

\textsuperscript{220} Article 2 (1) of the Environmental Information Directive.

\textsuperscript{221} Article 3 (1) of the Environmental Information Directive; “applicant” is broadly defined by Article 2 (5) as “any natural or legal person requesting environmental information”.

\textsuperscript{222} This exception may be specifically relevant to environmental VMS and Hazmat data.
f) the confidentiality of personal data and/or files relating to a natural person where that person has not consented to the disclosure of the information to the public, where such confidentiality is provided for by national or Community law;

g) the interests or protection of any person who supplied the information requested on a voluntary basis without being under, or capable of being put under, a legal obligation to do so, unless that person has consented to the release of the information concerned;

h) the protection of the environment to which such information relates, such as the location of rare species\(^{223}\).

695. It is also explicitly provided in the Environmental Information Directive that the aforementioned grounds for refusal “shall be interpreted in a restrictive way”, taking into account (for each particular case) the public interest served by disclosure (i.e. balance of interest between the application of a refusal ground and the public interest of disclosure). With regard to the exception relating to the confidentiality of personal data, it is explicitly provided that Member States shall ensure that the requirements of the Data Protection Directive are complied with.

696. It is also important to note that an instrument containing similar principles was adopted at Community level (i.e. with regard to access to environmental information held by Community institutions and bodies)\(^ {224}\).

697. Subject to a number of specifications, the Transparency Regulation is made applicable to requests by applicants for access to environmental information held by Community institutions and bodies\(^ {225}\). This includes applicability of the exceptions (i.e. grounds for refusal of access) provided for in Article 4 of the Transparency Regulation (also subject to certain specifications)\(^ {226}\).

\(^{223}\) Article 4 (2) of the Environmental Information Directive.


7 Conclusions

698. In order to integrate Europe’s maritime monitoring and surveillance systems, as foreseen in the action plan that accompanied the Communication setting out the European Commission’s vision for an Integrated Maritime Policy for the EU, a number of legal issues will first need to be addressed.

699. The most important legal issues seem to relate to confidentiality and personal data. In addition, data (security) policies may prohibit or restrict the sharing (or further use) of certain data.

700. As regards confidentiality, the basic obstacle is the explicit nature of the confidentiality provisions in some of the key instruments relevant to monitoring and surveillance, in particular the VTM Directive but also the VMS Regulation and the Control Regulation. It appears that a significant amount of maritime reporting and surveillance data is qualified and/or has to be treated as (commercially) confidential. As a consequence, the processing of these data will be affected by the duty of confidentiality and professional secrecy of the persons authorized to have access to the data.

701. Clearly, this confidentiality issue will have to be addressed in the case of data sharing. Given that these confidentiality provisions are contained in Community instruments, the ostensible ‘solution’ would be to modify the existing legislation (for instance, by removing, amending or otherwise specifying the references to “confidentiality” in Article 14 of the VMS Regulation, Article 37 of the Control Regulation, Article 24 of the VTM Directive and other Community instruments that refer to this). Alternatively, any proposed data sharing mechanism would need to ensure that recipients of the data are equally bound by confidentiality.

702. There are, however, as witnessed by the ongoing discussions in the European Parliament concerning the revision of the VTM Directive as well as the Commission’s original proposal itself, good public policy reasons why these confidentiality provisions were included in the first place. Indeed, the confidentiality of data seems to be at the heart of the debate over the amendments to the VTM Directive. The combination of VMS data with AIS data is a clear example of this.

703. This is not only a question of public policy but also a question of workability. The implementation of SafeSeaNet for example has in practice been hindered by confidentiality concerns at the Member State level. Again, legal security is one of the reasons why one of the proposed amendments to the VTM Directive aims at expressly establishing SafeSeaNet as a Community reference system.

227 Tables summarising these issues are attached as Annex D.
228 In this connection it is to be noted that the Control Regulation is currently being revised.
704. In any event, SafeSeaNet is in its current form at least primarily a mechanism for the exchange of data within a single sector namely the maritime sector. Extending data sharing beyond that sector will inevitably raise further challenges and questions concerning confidentiality given the range of additional actors that will be involved.

705. With regard to the use (including the sharing) of maritime data, sectoral legal provisions may impose specific restrictions (such as limitations on the purpose of the use or on the type of actors that may have access to the data). Further, it should be taken into account that, if the sourcing or sharing of data is taking place on a contractual basis (for instance, where data are acquired from commercial suppliers), such contracts may also contain specific restrictions (for instance, contractual provisions on intellectual property rights may limit the user’s right to reproduce, exploit and share the data).

706. In addition, the existing legal framework in relation to the protection of personal data will need to be properly integrated within data sharing initiatives involving this type of data. This Study has demonstrated that a significant number of maritime reporting and surveillance schemes may include personal data (i.e. data which allow to either directly or indirectly identify natural persons). Unlike the issue of confidentiality which could theoretically be resolved through changes to the relevant legal provisions, amending the existing data protection legislation in order to meet the objective of the maritime policy is clearly not an option.

707. Personal data protection law contains a number of significant use and purpose limitations to be complied with by those controlling and processing the data. In connection with the sharing of personal data, a number of specific safeguards will first need to be put in place in order to ensure that the basic principles of data protection law (such as the principle of proportionality) can be complied with.

708. The processing of personal data within the framework of a data sharing mechanism will therefore need to be based on appropriate legislative measures which will need to define the nature and the purpose(s) of the processing, the types of data involved, as well as the specific safeguards with regard to the protection of the data (such as the identification of the potential data controllers) and the rights of the data subjects.

709. The processing of personal data for military, State security and criminal law enforcement currently remains outside of the general legal framework for data protection. However, data protection may be addressed on an ad hoc basis in specific legal instruments in these fields, both at Community and Member State level. A specific legal framework for the sharing of personal data within the context of the EU’s third pillar (i.e. for the purpose of preventing and combating crime) is currently being debated. As a consequence, additional safeguards will be required in case it would be envisaged to share personal data between authorities falling within the scope of the existing legal framework for data protection (e.g. fisheries authorities) and authorities (currently) falling outside that scope (e.g. military, State security or law enforcement authorities).
710. Generally, in relation to data sharing, a number of key questions will need to be addressed. The first two questions are: what data is currently available and under which conditions? This Study seeks to provide answers to these questions.

711. To design the scope of future data sharing mechanisms, a third important question will first need to be answered: why is it considered necessary to share the data? In other words, in the context of maritime surveillance, what is the purpose of sharing the data?

712. Specifically, it is not appropriate to share data simply because the data are available and because it is technically possible to share them. A clearly defined purpose as to why the data is to be shared will be a fundamental pre-requisite to any data sharing mechanism. Especially in relation to the sharing of personal data, purpose-limitation and proportionality are fundamental principles which will need to be very carefully examined.

713. Obviously, the next question that will need to be answered is with whom the data are to be shared (and in each case why the data are to be shared with that particular entity). In other words, who are the designated authorities that will be entitled to control, disclose and receive the data? The various (potential) actors involved in data sharing will need to be clearly identified and described taking into account *inter alia* the scope of their respective competences.

714. The answers to the ‘why’ and the ‘who’ questions are beyond the scope of this Study, although this Study may have demonstrated the importance of addressing these questions appropriately.

715. Indeed, establishing or interconnecting data systems without putting in place an appropriate *legal framework* that addresses the aforementioned questions may give rise to a number of issues, such as the control over the quality of the data or the further use (or interpretation) of the data, as well as data security.

716. For the sake of the legal security of all the actors involved, it is suggested that any mechanism aiming at the cross-border exchange of data from various existing databases is made subject to a clear *legal framework* defining at least the nature of the data involved, the purposes (and the methods) of the exchange and the potential recipients of the data, as well as incorporating the necessary safeguards with regard to the confidentiality and security of (certain) data and the protection of personal data, where this may be relevant.
TECHNICAL SPECIFICATIONS TO SPECIFIC TASKS TO BE UNDERTAKEN IN THE FRAMEWORK OF LOT 2 OF FISH/2006/09 STUDIES IN THE FIELDS OF THE COMMON FISHERIES POLICY AND MARITIME AFFAIRS

WORK PACKAGE 1

LEGAL ASPECTS OF MARITIME DATA

A) MARINE ENVIRONMENTAL DATA
B) VESSEL SURVEILLANCE DATA

version
15 November 2007
GENERAL CONTEXT

In its recently adopted "Blue Paper" on an integrated EU maritime policy the Commission undertook to:

*take steps towards a more interoperable surveillance system to bring together existing monitoring and tracking systems used for maritime safety and security, protection of the marine environment, fisheries control, control of external borders and other law enforcement activities*

and

*take steps in 2008 towards a European Marine Observation and Data Network*

The sharing of data between countries and the use of data for purposes other than that for which it was first collected are central to both objectives.

SPECIFIC BACKGROUND TO THIS STUDY

Monitoring vessel movements and activities

There are many different systems for monitoring the movements of maritime traffic for particular purposes – such as Vessel Traffic Services (for safety of navigation), Automatic Identification Systems (for safety of navigation), Long Range Identification and Tracking (for security, search and rescue and other purposes), Vessel Monitoring System (for fisheries control), and other private (e.g. harbour approach) and military systems. The stakeholders consulted in the development of maritime policy were broadly in favour of integration methods. However there are a number of obstacles that need to be considered before proceeding further. These relate particularly to the confidentiality of the data and limits to its potential uses. The main Commission legislation is:

1. Commission Regulation (EC) No 2244/2003 which indicates that all EU fishing vessels over 15 metres must automatically report their positions to the flag state and the coastal state using the Vessel Monitoring System (VMS).
2. Directive 2002/59/EC established the obligation of an Community Vessel Traffic Monitoring system including a network of AIS base stations and Automatic Identification System (AIS) for almost all categories of ships
Furthermore in May 2006, the International Maritime Organisation (IMO) adopted amendments to the
International Convention of Safety of Life at Seas (SOLAS) introducing requirements for long range
identification and tracking of ships (LRIT), which will be operational by 31 December 2008.

**Marine environment**

Similarly there are many observation systems in place that cover various properties of the marine
environment. Some of these system make observations through remote sensing (platforms: satellites,
craft), some from land (coastal monitoring stations), or at sea (measurements from platforms at the
surface of the sea or submerged). The chain from instruction – setting up and operation of observation
system – observation – data management of data obtained can involve a mix of public and private
entities that establish between them specific internal rules governing the access and use rights for the data
generated. The reasons for the choice of a particular data policy may vary widely, and there may be trade-
offs involved: for instance, in some countries, agencies creating data may have been encouraged to
generate extra income through recovering the cost of its collection from users. This helps to meet the
collection costs but inevitably reduces the usage.

---


Common generic difficulties in networking data systems involve (legal) questions of ownership, data
policy, copy- or distribution rights, associated with the data derived from specific observation systems. As
indicated above, there is a range of situations between the "fully public" to the "fully private" ends of the
spectrum, with mixes not uncommon.

Improving the access to data will require first an assessment of the existing situation, partly to assess the
different practices used for particular types of data and partly to assess how far current practices for
marine data have adopted recent legislation on environmental data.

Some recent legislation that may further impact the situation includes:

1. Directive 2003/4/EC on public access to environmental information
2. Directive 2003/98/EC on the re-use of public sector information

The European Commission has also recently published, in the same spirit, a communication on "scientific
information in the digital age: access, dissemination and preservation" (COM(2007)56 of 14
February 2007).

**RELEVANCE OF STUDY TO WORK SPECIFIED IN FISH/2006/09 STUDIES IN THE FIELDS OF THE COMMON FISHERIES POLICY AND MARITIME AFFAIRS**

The study is relevant to Lot 2 "Legal Studies" activity 1 "Analysis of the existing law and proposals for
future law"

"Analysis of the existing law and proposals for future law. Studies could be asked to examine existing law affecting maritime affairs, and notably law that is indicated by respondents to the questions in the Green Paper as particularly problematic or that contradicts with maritime policy goals as set out in the Green Paper or that will be developed in the context of a future maritime policy. This could also include aspects of implementation, control, enforcement, administrative or commercial practices, decisions by judicial and quasi-judicial bodies or dispute settlement."

**EXPECTED OUTCOME**

The expected outcome is an understanding of the legal issues relating to:

1. sharing surveillance data that will feed into a Commission Communication on the subject.
2. access to marine environmental data that will help define how an operational system could be set up.

TASKS

The project has two main tasks which are largely independent of each other. Each task focuses on a different set of data. The purpose of the first is to support safe navigation and deter or detect illegal behaviour. It mainly consists of time-critical monitoring or surveillance of individual marine vessels. The main application of the second set of data is to understand the marine environment and human impact on it. It may be time-critical – for instance to provide early warnings of potentially hazardous data but the main focus should be on long-term data sets.

Task 1 Analysis of legal basis for collection of data, access to data and sharing of data and information in the context of maritime surveillance systems

Objective

The objective of this study is to understand the legal rights and restrictions on the sharing of real-time information collected within the framework of maritime surveillance systems, in particular consisting of

- reporting data from AIS, LRIT, VMS, etc.) and

- surveillance data (satellite, radar, stationary and mobile detection systems, cameras, intelligence etc., collected from the operational centres, mobile units, ports, border crossing points and other sources).

In particular it should be examined how the following data collected from different sources could be analysed, merged and used by one single Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) respectively within a common information sharing environment for the maritime domain:

- vessels (including size, type, purpose, registry, position, destination, cargo, as well as static data on history, ownership, characteristics etc.),
- people (including citizenship, criminal history, qualifications etc. of operators, passengers, crew, dock workers, agents, etc.),
- activities (including type, location, time of year, cargo, etc.).

Systems to be considered

The project would consider both civilian systems such as:

- Vessel Monitoring System for fisheries (VMS)
- SafeSeaNet, SSN in support of the EU directive 2002/59/EC including, pre notifications of arrival and dangerous cargo (Hazmat)
- Automatic Identification System (AIS)
- Long Range Information and Tracking (LRIT)
- Vessel Traffic Services (VTS)
- National border surveillance systems (e.g. SIVE system in Spain)

As well as military data from

- Finland/Sweden-led maritime picture arrangement that is expanding to cover the Baltic region and involves navies, coastguards and other agencies, such as Finland’s Maritime Authority.
- the Italian Navy-led 17 nation V-RMTC picture compilation arrangement
- NATO Maritime Command system to support its maritime-focussed counter-terrorism operations
- NATO's Maritime Situational Awareness concept
- Baltic sea submarine coordination centre

Work to be Done
The contractor should consider what data (position, course, cargo, etc) is transmitted and examine the relevant EU and international rules as to who has a right to the data and whether they can pass it on to third parties. Relevant legislation on personal data (such as the Data Protection Directives) or commercial secrecy should also be considered.

**Relevant Existing Studies**

The Commission services have prepared a set of documents describe the organisation of offshore activities in each littoral Member State and the existing cooperation and coordination in each of the maritime areas as well as the surveillance, monitoring and reporting systems currently in place in the EU. These will be provided to the consortium.

**Task 2 Analysis of legal basis for access to marine data for understanding the behaviour of seas and oceans.**

**Task 2.1 Collection of information on access rights and restrictions on marine data.**

1. Assess the adequacy of existing classification schemes such as ISO 19115
2. Develop a description of access conditions to marine data.
3. Investigate the rules applied and the legal background to a representative sample of marine data collected and distributed by public or semi-public national or regional organisations, universities (public and private), military bodies, trusts and enterprises. This analysis should also include situations where private bodies collect data on the basis of public licences or subsidies;
4. Provide the resulting analysis in the form of a database.

**Information to be Collected**

**Distribution Rights**

1. Distributors (national focal point, regional authorities, different institutions, other arrangement)
2. Further distribution (open, cannot be passed to third parties etc)
3. Restrictions on use (defined purposes only)
4. Restrictions on publication of results from data
5. Legal ownership of data
6. Legal basis for access restriction
7. Cost for complete dataset

**Characteristics of Data** (where appropriate or feasible use existing classifications eg ISO 19115)

8. Temporal precision of distributed data (minutes, hours, days, monthly, annual, sporadic)
9. Spatial precision of distributed data (grid size, zone area, map scale or number of point values)
10. Location (percentage of data covering own territorial waters, own jurisdictional waters (EEZ), high seas, jurisdictional waters and territorial seas of other countries.

The sampling should aim to cover a spread of organisation types, data types and countries that enable a broad overview on a European scale.

**Parameters to be analysed**

The parameters listed here are not intended to be a complete set of data that should be made available through the European Marine Observation and Data Network but rather a sample. The contractor should aim to determine access to a meaningful set of data that represents the different scientific disciplines – geology, oceanography, fisheries etc.

1. Bathymetry
2. Geological strata
3. Tide levels
4. Salinity
5. wave height
6. gravel extraction sites
7. vessel Monitoring System (VMS) reports
8. commercial fish landings
9. location of fishing activities
10. ice conditions
11. nutrients
12. phytoplankton
13. oil-spills
14. off shore structures and activities
15. underwater structures, pipe lines, cables ....

Organisational Coverage
1. Organisations in coastal states of the EU as well as Norway and Iceland
2. Helsinki Commission (HELCOM)

3. FAO (Food and Agriculture Organisation)
4. GOOS (Global Ocean Observation System (GOOS)
5. Eurogeosurvey
6. ICES (International Council for Exploration of the Sea)
7. EMSA (European Maritime Safety Agency)
8. IHO (International Hydrographic Organisation)
9. Other organisations if the contractor feels that they are of interest

Task 2.2 Analysis of general legal issues regarding access to data

Objective
The objective is to analyse the results of task 2.1, identify and classify legislation that is relevant to access to information and data and determine country by country, through examination of statutory and case law which laws have been applied and whether they have been enforced. Points that might be included are:

1. whether or not marine data is specifically included or excluded;
2. whether data held by military bodies is explicitly mentioned;
3. whether limitations are placed on the use to which the data is put and what these limitations are;
4. to what extent the limitations are compatible with relevant (especially European) legislation;
5. whether there is a charge for the data and if there are restrictions as to what may be charged for ("distribution only" or "collection and distribution")
6. what are the main obstacles to creating freer access to data.
7. what future institutional or legislative changes are in the pipeline that might change the current position.

The study should cover national laws (eg on Freedom of Information) as well as European Directives. (eg Directive 2003/4/EC on public access to environmental information or 2003/98/EC on the re-use of public sector information), Directive 2007/2/EC (INSPIRE)

Task 2.3 Analysis of regulatory data provided to Commission under Common Fisheries Policy

Objective
In addition to fisheries data collected under the Data Collection Regulation there are nearly 800 reporting obligations for Member States for parameters such as catch, effort and capacity. The Commission has developed a database indicating inter alia the legal basis for each obligation, the frequency of reports
and the transmission media (fax, e-mail, FIDES etc). The database is currently being validated by the services within DG-FISH who are responsible for monitoring the obligation. Approximately 90 obligations have been validated. The objective of this task is to clarify the legal conditions under which this data can be disseminated and published to third parties.

**Sampling**

The Commission will make available the necessary information from OBONT. It would seem unreasonable to ask for a complete analysis of all the reports. Firstly because there are so many and secondly because the legal conditions for dissemination may be homogeneous. The contractor should then sample a reasonable number in order to arrive at a confident conclusion concerning the whole sample.

**DELIVERABLES**

<table>
<thead>
<tr>
<th>Number</th>
<th>Related task</th>
<th>Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Task 1</td>
<td>A report on legal rights and restrictions on the sharing of real-time information collected within the framework of maritime surveillance systems</td>
</tr>
<tr>
<td>2</td>
<td>Task 1</td>
<td>A self-standing 15-page summary of the conclusions that is self-standing and easily understood by non-experts.</td>
</tr>
<tr>
<td>Related task</td>
<td>Deliverable</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Task 2.1</td>
<td>a database that indicates the legal status of marine data according to common criteria</td>
<td></td>
</tr>
<tr>
<td>Task 2.3</td>
<td>A spreadsheet that can be linked to the OBONT database indicating the access conditions for the reported data.</td>
<td></td>
</tr>
<tr>
<td>Task 2</td>
<td>A report including</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. A summary of the work done in task 2.1 in collecting information on current access to data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Description of the data and definitions used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Justification of the sampling strategy that should cover different data types and different authorities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Summary of the data that has been collected (parameters and countries) and indication where the information was obtained from.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. (from conclusions of task 2.2) identification and classification of legislation that is relevant to access to information and data and country by country summary through examination of statutory and case law of which laws have been applied and whether they have been enforced</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. A summary of the work done in task 2.3, including a justification for the sampling strategy and overall conclusions about access to data collected under reporting obligations to the EU</td>
<td></td>
</tr>
<tr>
<td>Task 2</td>
<td>A self-standing 15-page summary of the conclusions that is self-standing and easily understood by non-experts.</td>
<td></td>
</tr>
</tbody>
</table>
Annex B

Schedule of legal instruments consulted

**International Law**

**Law of the Sea and general**


3. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances which was concluded on 20 December 1988 in Vienna


6. Recommendation M.585-4* Assignment and use of maritime mobile service identities last updated in 2007


8. International Code for the Construction and Equipment of Ships Carrying Dangerous Chemicals in Bulk


10. SUCFIS Memorandum of Understanding, June 2004

11. Agreement Between Ireland, the Kingdom Of The Netherlands, the Kingdom Of Spain, the Italian Republic, the Portuguese Republic, the French Republic and the United Kingdom of Great Britain and Northern Ireland Establishing Maritime Analysis And Operations Centre - Narcotics dated 30 September 2007

* **Inmo Conventions and Instruments**

12. International Convention for the Safety of Life at Sea (SOLAS) of 1st November 1974

14. IMO Resolution MSC. 74 (69) (May 12, 1998)

15. International Ship and Port Facility Security Code

16. IMO Resolution MSC 202 (81) on 19 May 2006 amending SOLAS (LRIT)

17. Western European Particularly Sensitive Sea Area, West European Tanker Reporting System (WETREP) which was approved by resolution of the IMO MSC on 6 December 2004

18. IMO Resolution A.600(15)


20. Resolution A.857(20) adopted on 27 November 1997 on Guidelines for Vessel Traffic Services

21. Resolution A.917(22) adopted on Guidelines for the onboard operational use of shipborne Automatic Identification Systems (AIS)

22. Guidance Relating to the Implementation of SOLAS Chapter XI-2 and the ISPS Code issued by IMO MSC on 7 June 2004

NATO


25. Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces (London, 19 June 1951)


HELCOM


European Union

**European Community**


43. Resolution adopted by the Transport Council at its meeting in Luxembourg on 1-2 October 2007

44. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions examining the creation of a European Border Surveillance System (EUROSUR) COM (2008) 68 final.

45. Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

46. Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data


48. Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes (COM/2007/654final)


58. Report from the Commission on the implementation of the principles in EC Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents (COM/2004/45final)


60. Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM/2005/475 final of 4 October 2005)


67. Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European
databases in the area of Justice and Home Affairs (COM/2005/597final of 24 November 2005)

68. Data protection in the administration of the European Community, paper by Joaquin Bayo Delgado, Assistant European Data Protection Supervisor


70. Opinion of the European Data Protection Supervisor of 28 February 2006 on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability

71. Opinion of the European Data Protection Supervisor of 12 September 2007 on the Proposal for a Regulation of the European Parliament and of the Council establishing common rules concerning the conditions to be complied with to pursue the occupation of road transport operator

72. Opinion of the European Data Protection Supervisor of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas

73. Opinion of the European Data Protection Supervisor of 20 January 2006 on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences

74. Opinion of the European Data Protection Supervisor of 4 April 2007 on the initiative of (various countries) with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

75. Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes (OJ C-110/1 of 5 January 2008)

76. Preliminary Comments of the European Data Protection Supervisor of 3 March 2008 on (various Communications from the Commission, including on the creation of a European Border Surveillance System (EUROSUR) and the future development of the FRONTEX Agency)

77. Comments of the European Data Protection Supervisor of 10 March 2006 on the Communication of the Commission on interoperability of European databases

78. Order of the Court of 13 July 1990, J.J. Zwartveld and others, Case C-2/88


82. Judgment of the CFI of 13 April 2005, Verein für Konsumenteninformation, Case T-2/03

**National Legislation**

**Finland**
84. 1999 Freedom of Information Act
85. Territorial Surveillance Act (755/2000, as amended)

**France**
86. Decentralization Law of 2004

**Germany**
87. Grundgesetz

**Spain**
88. Ley Orgánica 2786, de Fuerzas y Cuerpos de Seguridad (Fundamental Law No. 2786 on Law Enforcement)
89. Order No. 26923 of 12 November 1998 of the Ministry of Agriculture, Fisheries and Food por la que se regula en España el sistema de localización de buques pesqueros vía satélite
90. Order No. 23943 of 22 December 2003 of the Ministry of Agriculture, Fisheries and Food por la que se regula en España el sistema de localización de buques pesqueros vía satélite y por la que se establecen las bases regulatorias de las ayudas para la adquisición e instalación de los sistemas de localización en los buques pesqueros

**United Kingdom**
91. Merchant Shipping Act 1995
92. Merchant Shipping (Registration of Ships) Regulations 1993, as amended
Annex C

Excerpt from the German Federal Maritime Responsibilities Act

§ 9e
(1) In so far as required for the fulfilment of a task in the terms of this Act, the body charged with carrying out this task is permitted to collect the following data:
1. identification data of a ship entered into a ship register or provided with an official radio frequency identification number (name of ship, register, sea and coastal radio frequency identification number, IMO ship identification number, official ship number, distinctive signal or radio paging signal, model, survey result, year of construction),
2. identification data of a recreational vessel (name, type of construction, year of construction, nationality identification plate, other official or officially recognised identification markings),
3. identification data of the owner, operator, charterer, captain of a ship or recreational vessel (surname and first name(s) or name, address),
4. information on person(s) onboard (surname and first name(s), citizenship, date and place of birth, type of identity document and identity document number, visa number if applicable, as well as ports of embarkment and disembarkment in the case of passengers),
5. identification data of the recognized organization in terms of Article 2 letter f of Council Directive 94/57/EC of 22 November 1994 on common rules and standards for ship inspection and survey organizations and for the relevant activities of maritime administrations (OJ L 319, p. 20), which has executed examinations or inspections necessary for the issuing of maritime certificates and certificates for required ship inspections or has itself issued maritime certificates (name, place of residence, branch office) and details of their recognition,
6. most recent port of departure, next port of call, destination port, position at the time of data collection, passage, speed, the standing, draught, planned route, and time of arrival of the ship at the next port as well as ship-related safety messages,
7. during the port state control or follow-up measures, such as the denial of port access, frequency, reasons and details of these measures and their suspension,
8. list of deficiencies during the flag state control,
9. cargo data,
10. with regard to ships in the terms of Regulation 2 para 1.1 of Chapter XI-2 of the Annex of the SOLAS Agreement which intend to make one or more port(s) of call in the Federal Republic of Germany, the safety-related data on the ship as stated in the Annex of the Guidance Document of the Maritime Safety Committee on the rules related to the transfer of safety-related data prior to the embarkment of a ship at the port (MSC/Circ. 1130 of 14 December 2004, Verkehrsblatt 2005 p. 143) in so far as the data is not covered by no. 1-9.

The data may also be collected with the aid and evaluation of automatic ship identification systems as well as the ship data recorder. Sentence 1 does not apply to vessels of the Federal Armed Forces.

(2) The data are only permitted to be used for the purpose for which they are collected. It is permitted for the data to be transferred to other official bodies if required for fulfilment of tasks in the terms of this Act or required to avert dangers or permitted by a sector-specific authorization basis. The data according to para 1 sentence 1 no. 1 to 10 are transferred to the Federal Police to ensure protection of federal territory as enforced by the border police; the transfer of data pertaining to para 1 sentence 1 no. 5, 8 and 9 is only undertaken on a case- to case basis upon request. In so far as a Land (federal state) attends to the tasks of the border
police in agreement with the Federation using its own resources or the performance of such
tasks has been passed on to the customs authority, sentence 3 accordingly applies to these
bodies. The identification data referred to in para 1 sentence 1 no. 1 and the data referred to in
para 1 sentence 1 no. 6 are also permitted to be transferred to port operators, ship reporting
services, port service operators, or other non-public bodies if it serves the fulfilment of tasks
in the terms of this Act. Sentence 1 also applies to a third party to whom the data are
transferred. The details of the data transfer are regulated by the Federal German Ministry of
Transport, Building and Urban Affairs in agreement with the Federal German Ministry of the
Interior without the sanction of the Bundesrat (Federal Council of Germany) in the form of a
statutory ordinance. In the statutory ordinance the third parties to whom the data are
permitted to be transferred shall be more closely defined.

(3) If data are transferred to a foreign or supranational or international public body or an
international organisation or organs and institutions of the European Communities, the body
to which the data are being transferred shall be informed that the transferred data are only
permitted to be used for the purpose for which the data are transferred. Data transfer which is
undertaken outside the scope of activities, which fully or partly fall under the scope of
European Community law, is not permitted in so far as the data subject has a legitimate
interest in excluding transfer, in particular if an adequate level of data protection is not
guaranteed at the body stated in the first sentence. Data on significant contraventions of
applicable international rules and standards pertaining to the seaworthiness of ships and the
protection of the marine environment are also permitted to be transferred if the body to which
the data are being transferred does not guarantee an adequate level of data protection.
Note: These tables are attached as a simple summary representation of findings. The reader is however referred to the text of the Study as to the substantive issues addressed.

### VMS

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vessel registration details</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio call sign</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Vessel name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External registration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Internal reference number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Activity details</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latitude</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Longitude</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Speed</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Course</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Trip number</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### AIS

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Static</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMSI</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call sign and name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IMO Number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Length and beam</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Type of ship</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Location of position fixing antenna</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Dynamic</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ship’s position with accuracy indication and integrity status</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Position Time stamp in UTC</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Course over ground (COG)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Heading</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Navigational status</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Rate of turn</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Voyage related</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ship’s draught</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>Hazardous cargo (type)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Destination and ETA</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Route plan (waypoints)</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

*Short safety-related messages*

Free format – as necessary - -
## LRIT

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity of Ship</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMO ship identification number</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MMSI</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Positional data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GNSS Position (latitude and longitude of ship)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>On-demand position reports</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Pre-scheduled position</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Time stamp</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date and time associated with GNSS Position</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Ship reporting systems

#### Port entry

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ship identification</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call sign</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IMO ID number/MMSI</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Port of destination</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimated sailing times</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ETA at port of destination/pilot station</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ETD</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Total number of persons on board</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## Mandatory ship reporting systems

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential issue</th>
<th>personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of system</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>A. Ship (name, call sign or ship station ID and flag)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>B. Date and time</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>C. Position</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>D. True bearing and distance from a clearly identified landmark</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>E. True course</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>F. Speed</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>G. Port of departure</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>H. Date, time and point of entry into the system</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>I. Destination and ETA</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>J. Whether pilot on board (deep sea or local)</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>K. Date, time and point of exit from system or arrival at ship’s destination</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>L. Route information (intended track)</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>M. Full names of radio-communication stations/frequencies guarded</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>N. Time of next report</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>O. Maximum present static draught</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>P. Cargo and brief details of any dangerous harmful substances and gases that could endanger persons or the environment</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Q. Brief details of defects, damage, deficiencies or other limitations</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>R. Description of pollution/dangerous goods lost overboard</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>S. Weather &amp; sea conditions prevailing</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>T. Details of the name and particulars of ship’s representative or owner or both for provision of</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Information</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-----</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td>U. Details of length, breadth, tonnage and type of vessel as required</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>V. Doctor, physician’s assistant, personnel without medical training</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>W. Total number of persons onboard</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Y. Request to relay to another system</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Z. End of report</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
## Hazmat

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A. General information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) Ship identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call sign</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IMO number/MMSI</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(b) Port of destination</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(c) For a ship leaving a Port in a Member State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimated time of departure from port/pilot station</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Estimated arrival at port of destination</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(d) For a ship coming from a port outside the EU and bound for a port in a Member State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estimated time of arrival at the port of arrival/pilot station as required by the competent authority</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(e) Total number of persons on board</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>B. Cargo information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) Correct technical names of dangerous or polluting goods using UN numbers where they exist, IMO hazard class in accordance with IMDG, IBC &amp; IGC codes, quantities of such goods, location on board, identification number if being carried in cargo units other than tanks</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(b) Confirmation that a list or manifest or appropriate loading plan giving details of the dangerous/polluting goods and their location on the ship is on board</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(c) Address from where detailed information about the cargo may be obtained</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data type</td>
<td>Confidential data issue</td>
<td>Potential personal data issue</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td><strong>A. General information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) Ship identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call sign</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IMO number/MMSI</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(b) Position</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(c) Port of departure</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(d) Port of destination</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(e) Address from which information on goods on board can be obtained</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(f) Total number of persons on board</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>B. Details of the incident</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(a) any incident or accident affecting the safety of the ship, such as collision, running aground, damage, malfunction or breakdown, flooding or shifting of cargo, any defects in the hull or structural failure;</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>(b) any incident or accident which compromises shipping safety, such as failures likely to affect the ship's manoeuvrability or seaworthiness, or any defects affecting the propulsion system or steering gear, the electrical generating system, navigation equipment or communications equipment</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>(c) any situation liable to lead to pollution of the waters or shore of a Member State, such as the discharge or threat of discharge of polluting products into the sea;</td>
<td>Yes*</td>
<td>No</td>
</tr>
</tbody>
</table>
(d) any slick of polluting materials and containers or packages seen drifting at sea

<table>
<thead>
<tr>
<th></th>
<th>Yes*</th>
<th>No</th>
</tr>
</thead>
</table>

* Subject to the duty to broadcast information for safety reasons and to alert competent authorities in other Member States.
Port security notification requirements

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>That the ship possesses a valid security Certificate</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>The security level at which the ship is operating</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>The security level at which the ship operated in the previous port</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Any special security measures taken by the ship in the previous port</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>That the appropriate security procedures were maintained during any ship to ship activity within the last 10 calls at port facilities</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Other practical security information</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Information contained in the Continuous Synopsis Record</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Location of the ship at the time the report is made</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ETA in port</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Crew list</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>General description of cargo aboard the ship</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Passenger list</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Information regarding who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Summary Table

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Legal basis</th>
<th>Purpose</th>
<th>Potential data law issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EC Law</td>
<td>International Law</td>
<td>National Legislation</td>
</tr>
<tr>
<td>Reporting regimes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMS</td>
<td>VMS/Control Regulations</td>
<td>No.</td>
<td>No.</td>
</tr>
<tr>
<td>AIS</td>
<td>VTM Directive</td>
<td>SOLAS</td>
<td>Yes</td>
</tr>
<tr>
<td>LRIT</td>
<td>No</td>
<td>SOLAS</td>
<td>Not yet</td>
</tr>
<tr>
<td>Ship reporting systems</td>
<td>VTM Directive</td>
<td>SOLAS</td>
<td>Yes</td>
</tr>
<tr>
<td>Hazmat</td>
<td>VTM Directive</td>
<td>SOLAS</td>
<td>Yes</td>
</tr>
<tr>
<td>Accident/Incident reporting</td>
<td>VTM Directive</td>
<td>SOLAS</td>
<td>Yes</td>
</tr>
<tr>
<td>Port security notification regulation</td>
<td>Port Security Regulation</td>
<td>SOLAS</td>
<td>No</td>
</tr>
<tr>
<td>Schengen Border Code</td>
<td>Schengen Border Code</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Surveillance Schemes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIVE</td>
<td>N/A</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VTS</td>
<td>VTM Directive</td>
<td>SOLAS</td>
<td>Yes</td>
</tr>
<tr>
<td>Clean Sea Net</td>
<td>Limited</td>
<td>No</td>
<td>No (contractual)</td>
</tr>
</tbody>
</table>
Schengen Notification requirements

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ship (other than cruise ship)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crew list</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Passenger list</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Presence of stowaways</td>
<td>No</td>
<td>No – provided not named</td>
</tr>
<tr>
<td><strong>Cruise ship</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Crew</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name and surname</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Date of birth</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Nationality</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Number and type of travel document &amp; visa if applicable</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Passengers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name and surname</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Date of birth</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Nationality</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Number and type of travel document &amp; visa if applicable</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### SIVE

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra red images</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Radar images</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Video images</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### VTS

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra red images</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Radar images</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Video images</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Clean Sea Net

<table>
<thead>
<tr>
<th>Data type</th>
<th>Confidential data issue</th>
<th>Potential personal data issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite image</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>AIS data</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>