Legal aspects of maritime monitoring & surveillance data
Summary report
“Socio-economic studies in the field of the Integrated Maritime Policy for the European Union”

- The role of Maritime Clusters to enhance the strength and development in European maritime sectors – Executive summary
- Legal aspects of maritime monitoring & surveillance data – Summary report
- Legal aspects of marine environmental data – Summary report
- Legal aspects of maritime spatial planning – Summary report
- The economics of climate change adaptation in EU coastal areas – Summary report

To be published:
- Study on tourist facilities in port
- Legal aspects of shipping in Arctic
- EU role in international organisations

Manuscript completed in October 2008.

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2009
© European Communities, 2009

The content of this report does not reflect the official opinion of the European Communities. Responsibility for the information and views expressed therein lies entirely with the authors. Reproduction is authorised provided the source is acknowledged.

© Cover pictures: iStock

Printed in Belgium

Printed on white chlorine-free paper
Legal aspects of maritime monitoring & surveillance data

Summary report
1 Introduction

Maritime monitoring and surveillance data are 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. Changes in the focus and scope of maritime surveillance over recent years have been accompanied by technological developments that permit the acquisition, processing and exchange of large quantities of data in real time or near real time.

The background to this Study is the ongoing development of the European Union (EU) Maritime Policy. The year-long public consultation exercise for the Maritime Policy revealed broad stakeholder support for further integration of maritime monitoring and surveillance data.

On 10 October 2007 the European Commission adopted a Communication\(^1\) setting out its vision for an Integrated Maritime Policy for the EU, together with a detailed action plan\(^2\) 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.

As provided for in the action plan, the Commission is due to adopt 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 was commissioned to provide a better understanding of the legal rights and restrictions that apply to the use and sharing of maritime monitoring data relating to vessels, individuals and activities. The Study focuses on three different types of scheme:

- reporting regimes where data must be actively reported by a person or vessel;
- surveillance systems where data are gathered in respect of a person or vessel without the active participation of the latter; and
- data sharing mechanisms for the exchange of maritime monitoring and surveillance data.

The basic questions asked in this Study are: (a) what data are collected/used/shared?; (b) what is the legal basis for this?; (c) why are the data collected/shared?; (d) who is entitled to the data?; and (e) what are the legal constraints on sharing such data between public agencies?

After analysing the different schemes, the Study goes on to examine the potential legal barriers to the exchange of maritime monitoring and surveillance data primarily on the basis of international and European Community (EC) law. Finally, some preliminary conclusions are presented.

2 The Law of the Sea

Although the focus of this Study is on the area of law known as ‘data law’, maritime monitoring and surveillance takes place against the background of the sea, and the branch of public international law known as the Law of the Sea. Two elements of the Law of the Sea are of particular relevance: the provisions on maritime zoning contained in the United Nations Convention on the Law of the Sea (LOSC) and the notion of the nationality of ships.

As regards surveillance activities, in summary, a coastal State has the exclusive right to undertake monitoring and surveillance within its territory including its territorial sea which, pursuant to LOSC, may extend up to 12 nautical miles (nm) from the ‘baseline’ (usually the low water mark). A coastal State also has the exclusive right to undertake monitoring and surveillance in connection with: (a) the economic exploitation and exploration of its Exclusive Economic Zone (EEZ) (including activities relating to the exploitation of living and non-living resources as well as energy production) which may extend up to 200 nm from the baseline; and (b) the exploitation of the sea bed and sedentary species on its continental shelf (which may in certain circumstances extend beyond 200 nm from the baseline).

Furthermore, 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 freedom of the high seas by ships flying a foreign flag. Finally mention can also be made of Search and Rescue (SAR) regions which have a purely functional purpose and do not have any impact on maritime zones claimed pursuant to LOSC.

The ascription of nationality to ships is one of the most important means by which public order is maintained at sea. The nationality of a ship indicates which State is entitled to exercise jurisdiction over the vessel – the ‘flag State’ – and thus which State is responsible for such vessel under international law.

Beyond rather brief provisions on ship nationality, LOSC leaves it to each state to fix the conditions for the grant of their nationality to vessels by means of registration. In practice ships can change nationality somewhat rapidly and with relative ease. Due in part to the variable quality of ship registers in 1987 the Ship Identification Scheme was introduced by the International Maritime Organisation (IMO), the United Nations agency responsible for shipping, and (with a limited number of exceptions) became mandatory in 1996 for all propelled merchant ships of 100 gross tonnage. IMO numbers are unique and are never reused or re-assigned. As regards registration at national level this is a matter for national law and practice and the possibility that two vessels flying the same flag may share the same name cannot necessarily be ruled out.
3 Reporting regimes

Because reporting regimes impose a legal reporting obligation it is relatively easy to determine what legal rules apply as evidently this must be specified in law.

3.1 Vessel monitoring system (VMS)

In connection with the implementation of the common fisheries policy each Member State is required pursuant to the Control Regulation (EC) 1489/97 and the VMS Regulation (EC) 2244/2003 to establish a VMS whereby data relating to the identification, position, speed and course of its fishing vessels above 15 metres in length can be transmitted at all times by satellite to a fisheries monitoring centre (FMC).

These data include three unique identification numbers: (a) the Community Fleet Register number of each vessel which in turn correlates with details contained in the national fishing boat registers that must be maintained by each Member State; (b) a national register number; and (c) the external or side number of the vessel. In addition, for most vessels, the radio call sign number will be unique. This data is collected to ensure the effective monitoring of the activities of fishing vessels.

Each flag Member State is entitled to receive VMS data through its FMC. In addition a coastal Member State is entitled to receive data from the flag State FMC in respect of a foreign fishing vessel in its waters. The European Commission is also entitled to obtain remote on-line access on specific request. Practice as regards sharing of VMS data at national level beyond the FMC varies among Member States.

3.2 Automatic Identification System (AIS)

AIS is a ship-born mechanism that automatically provides for the exchange of data between ships as well as coastal stations. This data includes: (a) fixed data such as the unique maritime mobile service identity (MMSI), call sign and name, IMO number and details of the ship; (b) automatically generated dynamic navigational data including details of the ship’s position, course and speed over ground and navigational status; and (c) manually entered voyage data. The rate of data exchange increases as a ship gains speed.

The fitting of AIS is mandatory for all vessels of 300 gross tonnage and above on international voyages, cargo ships of 500 gross tonnage and above and passenger ships irrespective of size. Warships and government owned vessels are exempt. The basic obligation to fit and use AIS is imposed by Regulation 19 of Chapter 19 of the International Convention for the Safety of Life at Sea (SOLAS). Furthermore the Vessel Traffic Monitoring Directive 2002/59/EC (the ‘VTM Directive’) requires any ship calling at the port of a Member State to be fitted with AIS. The purposes of AIS include promoting the safety of navigation, collision avoidance, enabling coastal States to obtain information about ships and their cargoes and as a VTS tool (see below).

Implicit in the structure of AIS is that other vessels within transmission range are entitled to AIS data as are the monitoring stations of coastal States. Furthermore the VTM Directive provides for the exchange of AIS data between Member States. In addition, because AIS is
transmitted un-encrypted over open frequencies, there is nothing to prevent anyone with suitable equipment from receiving it.

3.3 **Long Range identification and Tracking of Ships (LRIT)**

LRIT is a new long-range vessel monitoring system which also requires the periodic transmission of the name and course of vessels. However the data is transmitted only at six hourly intervals and the transmissions take place by satellite meaning that LRIT is a closed system.

The legal basis for LRIT is contained in Regulation 19-1 of Chapter V of SOLAS which provides that the following, providing they are parties to SOLAS, are entitled to LRIT data: (a) the flag State at all times; (b) a port State where a ship has indicated its intention to enter a port in that State; and (c) a coastal State in respect of a ship within 1,000 nm of its coast (unless the ship is in the waters of its flag State). LRIT is not yet fully operational.

3.4 **Ship reporting systems**

Many ship reporting systems are found in European waters. These include: (a) mandatory systems that apply to specific stretches of water; (b) a general obligation to notify information to the authority of the port of destination; and (c) reporting schemes relating to VTS (see below).

Reporting systems are addressed in Regulation 11 of Chapter V of SOLAS. In addition, Article 4 of the VTM Directive requires the operator, agent or master of a ship bound for an EU port to notify the relevant port authority within a specified time scale: (a) ship identification (name, call sign, IMO or MMSI number); (b) port of destination; (c) estimated time of arrival; and (d) total number of persons on board.

Mandatory ship reporting systems, which in general terms require IMO approval if they involve more than one country, are also addressed in the VTM Directive by reference to the relevant SOLAS provisions. Data to be reported typically include ship identification and type, navigation information (course speed), as well as details of cargo type and the total number of persons on board. In broad terms the purpose of such systems is to promote the safety of navigation and to enable the responsible authorities to respond effectively in the event of an incident.

3.5 **Notification of dangerous/polluting goods aboard ships (Hazmat)**

The Hazmat reporting requirements are set out in the VTM Directive and require the prior notification of dangerous or polluting goods carried on vessels departing from Member State ports or entering such ports from outside the Community.

The information to be notified to the designated Member State competent authority includes ‘General Information’ (ship identification, port of destination, estimated departure/arrival times and total number of persons on board) and ‘Cargo Information’ using UN numbers, IMO hazard classes etc.
3.6 Incident and accident reporting requirements

Beyond the duty imposed by Chapter V of SOLAS on the master of every ship to notify every ship it meets of ‘dangerous conditions’, Title III of the VTM Directive imposes a number of reporting requirements concerning incidents and accidents at sea in order to prevent or mitigate any significant threat to maritime safety, the safety of individuals or the environment.

‘Dangerous conditions’, under SOLAS, include dangerous ice, direct dangers to navigation, tropical and other storms but there is no prescribed format for ‘danger messages’.

The incidents and accidents to be reported pursuant to the VTM Directive include any accident affecting the safety of the ship, or shipping safety in general as well as potential and actual pollution incidents. Such data is to be transmitted to the relevant coastal station which must then take appropriate measures to forward/broadcast the information.

3.7 Port security notification requirements

The Port Security Regulation (EC) 725/2004 establishes Community measures to enhance the security of ships used in international trade, domestic shipping and associated port facilities in the face of threats of intentional unlawful acts.

It also seeks to give effect at Community level to measures agreed at the Diplomatic Conference of IMO in 1992 through the addition of a new Chapter XI-2 to SOLAS as well as the adoption of the International Ship and Port Facility Code (ISPS Code).

This complex body of law requires inter alia the master of any ship intending to enter a port within the EC to transmit various data to the competent authority for maritime security of the port State concerning, amongst other matters, the security level at which the ship is operating as well as details of the crew, any passengers and the ship’s cargo.

3.8 Schengen notification requirements

Crew and passenger notification requirements are also imposed on the captains of ships entering ports within the Schengen Area of the EU (i.e. not including Ireland and the UK) in accordance with the Schengen Borders Code.

Lists of the crew and passengers must be provided in duplicate to the border guards at the latest on the ship’s arrival in port. Thereafter, a signed copy of the list is returned to the captain and must be retained while the ship remains in port. Changes to the composition of the crew must be promptly notified to the competent authorities. Modified rules may apply with respect to certain types of vessel including cruise ships, pleasure boats and coastal fishing vessels.
4 Surveillance systems

A range of different surveillance techniques are typically used under this heading including visual sightings, still cameras, closed circuit television (CCTV), radar and infra red imaging. While the main limitation of such systems lies in the limited information that can be provided, they nevertheless play an important role in building up a maritime picture: (a) in cases where data is not provided under a reporting regime (whether deliberately or not); (b) in respect of (typically smaller) vessels that are not subject to a reporting regime; and (c) due to their immediacy and, in some cases, greater accuracy.

4.1 Military surveillance systems

The gathering of surveillance data is inherent to the role of Europe’s navies for defence purposes, which since 2001, includes defence against terrorism.

Assessing what surveillance data is actually collected is a difficult task: the data itself is usually classified as is information about acquisition mechanisms. Nevertheless it is possible to surmise that maritime surveillance data is gathered through: (a) physical observation from military vessels and aircraft; (b) unmanned vehicles and drones; (c) remote sensing; (d) coastal radars; and (e) underwater sensors. As will be seen below Europe’s navies typically also make use of civilian monitoring and surveillance data.

4.2 Sistema Integrado de Vigilancia Exterior (SIVE)

SIVE is a Spanish coastal surveillance system operated by the Guardia Civile. Originally designed to focus on small vessels carrying illegal immigrants it is used to detect, identify and intercept a range of illegal activities around Spain’s maritime frontiers. It is based on a network of fixed stations and mobile units that make use of still cameras, CCTV, radar and infra-red sensors. The data (video images, radar tracks and infra-red images) are transferred by secure internet to provincial control centres. There is no specific legal basis for SIVE – it derives from the basic mandate of the Guardia Civile. At present the data is used only by the Guardia Civile.

4.3 Vessel traffic services (VTS)

VTS are shore based-systems which range from the provision of information messages to the extensive management of maritime traffic. There are two basic types of VTS: (a) port VTS which are concerned primarily with traffic management in/around a port; and (b) coastal VTS which deal with traffic passing through a specific area.

Usually, on entering a VTS area the master of a ship must first report to the authority responsible for the VTS. He must then monitor a specific radio frequency for navigational or other warnings. The activities of a ship within a VTS area are, however, usually monitored by the VTS authority using radar, AIS and in some cases radio direction finders (RDF) and remote video cameras.

In terms of international law the legal regime for VTS is contained in Regulation 12 of SOLAS supplemented by guidelines adopted pursuant to IMO Resolution A.857(20) of 27 November 1997. At EC level, VTS is addressed in Articles 8 and 9(3) of the VTM Directive. The guidelines
state that the purpose of VTS is to improve the safety and efficiency of navigation, safety at sea and the protection of the marine environment, offshore installations etc from possible adverse effects of maritime traffic.

4.4 CleanSeaNet

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). EMSA obtains radar satellite images from a commercial satellite provider in response to requests from Member States.

5 Data sharing mechanisms

A range of mechanisms currently exist for sharing maritime monitoring and surveillance data at national and international level. While some national level mechanisms enable the sharing of data among different agencies for a range of different purposes, at the international level such mechanisms are single purpose.

5.1 National data sharing mechanisms

The French SPATIONAV information system is designed to collect and compile data generated by a range of sensors to assist maritime operational centres in the performance of their duties. The principal partners are the Navy, the Directorate of Maritime Affairs and the Customs Department. SPATIONAV, which makes use of data provided by coastal observation stations and AIS, operates alongside another mechanism, TRAFIC 2000, which was developed to implement the VTM Directive. The primary role of TRAFIC 2000 is to provide the authorities responsible for maritime security the data necessary to assess risks to security, safety and the environment from vessels, including those carrying dangerous or polluting goods. The system is intended to be integrated with SafeSeaNet (see below).

Finland has a well developed maritime data exchange mechanism the principal actors in which are the Navy, the Frontier Guard and the Maritime Administration. Pursuant to a 1993 inter-agency memorandum, AIS and VTS data, including data from the GOFREP reporting system are sent by the Maritime Administration to the Navy as are data gathered by the Frontier Guard from its patrol vessels and aircraft and sensors. This data is then compiled with the Navy’s own classified data to create a real-time maritime picture. Data is then distributed to the two agencies in accordance with their needs. It is also supplied to a range of ‘secondary’ agencies including the environment ministry, customs, police and rescue service.

5.2 Regional AIS data sharing agreements

The HELCOM AIS Network enables the real time sharing of AIS data among the parties to the 1992 Helsinki Convention (Denmark, Estonia, EC, Finland, Germany, Latvia, Lithuania, Poland, Russia and Sweden) and Norway. The North Sea Data Exchange, developed with the assistance of INTERREG III undertakes a similar function for North Sea countries Norway, Sweden, Denmark, the Netherlands, Belgium and the UK and a similar network is currently planned for the Mediterranean.
5.3 SafeSeaNet

SafeSeaNet is a data exchange system, based on an index server, developed by EMSA to support the implementation of elements of the VTM Directive (relating to port, HAZMAT, ship and alert notifications). SafeSeaNet is not specifically referred to in the VTM Directive although some of the reporting requirements are. It is envisaged that SafeSeaNet, which is not yet fully operational will also be used to distribute LRIT data. One of the reasons for its slow implementation has been concerns at the Member State level over data security and the lack of a clear and binding data policy for SafeSeaNet.

5.4 Commercial AIS data sharing mechanisms

Because, AIS data is unencrypted and broadcast over publicly available wavelengths, a number of commercial companies have successfully established web-based AIS data sharing mechanisms. The first such service, and one of the largest, is AIS Live which is owned by Lloyds Register Fairplay Limited. Access to this service is by subscription.

5.5 Finland/Sweden

Since 2006 the Swedish and Finnish navies have routinely exchanged their respective compiled maritime pictures on the basis of a 2005 memorandum of understanding. The data shared is classified and is safeguarded in accordance with applicable national legislation.

5.6 Maritime Analysis and Operations Centre – Narcotics (MAOC-N)

MAOC-N, which is based in Lisbon, is a law enforcement centre that coordinates the maritime interdiction of illegal drugs trafficked on the high seas. It was established in 2007 on the basis of an agreement between Ireland, the Netherlands, Spain, Italy, Portugal, France and the UK. Data is gathered from a range of sources including AIS and classified intelligence.

5.7 Virtual Maritime Traffic Centre (V-RMTC)

The V-RMTC is a virtual network connecting the operational centres of a number of navies that enables the sharing via internet of unclassified information on merchant shipping. Coordinated by the Italian Navy, it was established in 2006 pursuant to an Operational Agreement between some 15 countries with naval interests in the Mediterranean.

5.8 NATO – Marine Situational Awareness (MSA) Concept

NATO’s Maritime Safety and Security Information System (MSSIS) is based around AIS data, provided by NATO-member States and a number of non-NATO States, which the location and movement of some 10,000 ships to be tracked each day. This data is then analysed using a range of software analysis tools, some of which make use of commercial and open source databases, to identify potential anomalies. The analysed data is then fed into NATO’s Maritime Command and Control Information System which also includes intelligence data, classified data and the real-time location of NATO vessels.

8
5.9 Other planned data sharing mechanisms

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 lives at sea, and increasing the internal security of the EU. The communication proposes that in a first phase existing surveillance systems and mechanisms should be interlinked and streamlined and that a secure computerised communication network should be established in order to permit real-time data exchange 24 hours a day between centres in the Member States as well as FRONTEX. Phase 2 is concerned with the development and implementation of common tools and applications for border surveillance at EU level while Phase 3 will seek to integrate all existing sectoral systems which are reporting and monitoring traffic and activities in European waters into a broader network to allow border control authorities to take advantage of the integrated use of these various systems.

Meanwhile the European Defence Agency (EDA) began work some two years ago on its Maritime Surveillance Project (MARSUR) in order to explore the needs and requirements for a purely European naval surveillance system.

6 Potential legal restrictions

As if mirroring the complexity of the various monitoring and surveillance schemes described above, this is a complex area of law.

6.1 Confidentiality and commercial secrecy

The confidentiality of certain data can be a potential barrier to its exchange. Confidentiality can originate: (a) by law due to the inclusion of express legal provisions to this effect; (b) or on the basis of contractual provisions. A number of the legal instruments cited in this report contain examples of confidentiality provisions.

For example the various regulations that establish the legal framework for VMS contain references to the confidentiality of VMS data, the requirements for such data to be ‘treated in a confidential manner’ and statements to the effect that such data are covered by ‘professional secrecy’. Such provisions do not constitute an obstacle, as such, to the exchange of data between Member State FMCs and the European Commission in accordance with the specific mechanisms described in this report. However, recipients of such data are under a duty of confidentiality and in general terms may not, therefore, disclose it to third parties not specifically mentioned within the relevant legal framework.

Similar provisions are found in the VTM Directive with the effect that while data must be exchanged between relevant Member State authorities in accordance with the requirements of the directive, all recipients are themselves under a duty to keep the data confidential and thus they may not share such data with non-designated authorities.

Other examples of confidentiality provisions can be found in the Port Security Regulation, the provisions in SOLAS on LRIT and the Schengen acquis.
With regard to confidentiality provisions imposed by contract one example is the standard agreement of Lloyds Register Fairplay Limited relating to AIS Live which imposes a duty of confidentiality on users and effectively prohibits unauthorised third party re-use. Similar provisions are to be found in the end user licence for CleanSeaNet including a purpose limitation, the effect of which is that Member States may use the data solely for the purpose of oil spill monitoring. Typically agreements of this type also include provisions on the protection of the data supplier’s intellectual property rights.

6.2 Processing of personal data

Another potential restriction on data sharing may arise if the data involves ‘personal data’, in which case data protection laws will, in principle, apply. The two main instruments of EC data protection law are the Data Protection Directive 95/46/EC and the Data Protection Regulation 45/2001/EC. The Data Protection Directive seeks to enable the free flow of data between Member States, by harmonising national rules, while at the same time ensuring that the fundamental rights of individuals, notably the right to privacy, are protected with regard to the processing of data. The Data Protection Regulation seeks to apply the same basic principles to Community institutions.

The concept of ‘personal data’ is very broadly defined in the Data Protection Directive. In outline it means any information relating to an identified or identifiable natural person. An ‘identifiable person’ is further defined as one who can be identified directly or indirectly by reference to an identification number or one or more factors specific to his physiological, mental, economic, cultural or social identity. Although this broad definition has led to some uncertainty, particular items of information such as a telephone number, car registration number, social security number or passport number can be sufficient to render someone directly or indirectly identifiable and thus may, in the context of a particular situation, amount to personal data. Furthermore, in certain circumstances information on legal persons may also amount to personal data, for example where the name of a legal person derives from that of a natural person.

Consequently while it seems reasonable to conclude that the name of a vessel may not as such be sufficient to directly identify a (natural) person owning a vessel the unique combination of the vessel name with other data elements, such as a unique vessel registration number, that enable the identification of a single person (vessel owner, captain, crew etc.) may amount to personal data. Furthermore, pictures, including CCTV images and other visual data may also be considered personal data if they permit the identification of a natural person.

Taking the above into account, analysis of the maritime monitoring and surveillance data described above leads to the conclusion that they could potentially involve personal data (e.g. where data concerns a fishing vessel identification number, a licence number or external registration number or other unique identifiers that can lead directly or indirectly to the identification of a natural person). While in the large majority of cases the owner or agent of a vessel will be a legal person this may not always necessarily be the case. Various references made in the legal instruments described in this Study (for example in the Community fisheries legislation, the Port Security Regulation and the Schengen Borders Code) suggest that data protection concerns were taken into account from the outset.
In addition to the broad concept of personal data the definition of the ‘processing of personal data’ is equally broad and basically covers any type of manipulation of data that can be considered person data.3

As the schemes described in this Study may involve the processing of personal data it is necessary to examine the main restrictions on the sharing of such data pursuant to data protection law. First of all, the processing of personal data needs to be legitimate. The Data Protection Directive and Regulation define the grounds for such legitimacy, including if the processing is in the public interest or in the exercise of official authority.

The ‘purpose-limitation’ is one of the cornerstones of data protection law: personal data can only be processed for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. 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 (principle of proportionality).

Personal data can therefore, 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.

From the perspective of data protection law, the processing of personal data needs to remain restricted to: (i) the competent authorities or organisations designated for such processing; and (ii) the purposes laid down by the relevant laws or regulations that allow (or impose) the processing.

A number of examples of the purpose-limitation for data processing can also be found in the maritime sector legislation described in this Study. The overall effect is that 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, competence of the receiving authority. In other words the purpose of the processing of data is therefore of crucial importance. The purpose limitation has other impacts including as regards storage or retention: personal data may not be kept in a form that permits the identification of data subjects for longer than is necessary for the purpose for which the data were collected or for which they are further processed. It follows that data collected for one purpose must be deleted as soon as that purpose is fulfilled.

As regards data sharing another important principle of data protection law is that data may not be transmitted to recipients outside the European Economic Area (EEA) which do not ensure an adequate level of protection. Very few non-EEA countries currently meet these criteria. However data transfers outside the EEA may take place if adequate safeguards are put in place as a result inter alia of appropriate contractual arrangements.

Data protection law also: imposes a duty on controllers of personal data to implement adequate security measures and to keep such data confidential; and confers certain rights on

---

3 ‘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’.
data subjects (such as the right to access and consult the data and to request rectification of inaccurate data).

Finally it is important to note that data protection legislation does not automatically apply to the processing of all personal data. Exceptions include the processing of personal data in the course of an activity that falls outside EC law (e.g. second and third pillar activities such as the common foreign and security policy and police and judicial cooperation in criminal matters) as well as processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law (although there is currently a proposal to regulate the processing of personal for third pillar activities).

6.3 Data policies of public authorities

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. Data security and classification policies may be especially relevant for military authorities.

6.4 Re-use of public sector information

The Public Sector Information Directive 2003/98/EC, which provides for minimum rules applicable in all the Member States as to the re-use of public sector information resources, may potentially be relevant to the sharing of maritime monitoring and surveillance data in cases where bodies involved in the sharing of such data operate under a semi-privatised structure or in situations where public sector bodies (trans)act themselves in a commercial sphere.

6.5 Access to public sector documents

Potential restrictions to data access may also derive from instruments at EU and Member State level concerning public access to data and which usually contain a number of grounds under which such access may be refused.

At EC level the principal instrument is the Transparency Regulation (EC) 1049/2001 which regulates public access to documents held by Community institutions. The Transparency Regulation seeks to balance the basic principle that all documents should be accessible to the public with the need in certain circumstances to protect certain public and private interests by way of exception to this rule. To this end a number of mandatory exceptions are provided for (including those relating to public security, defence and military matters) along with other refusal grounds which apply unless there is an overriding public interest in the disclosure. Member States may request an institution not to disclose a document without its prior agreement and, in addition, the regulation contains specific provisions regarding ‘sensitive documents’ classified as ‘TOP SECRET’, ‘SECRET’ and ‘CONFIDENTIAL’. If maritime monitoring and surveillance data were to be so classified this might constitute a barrier to their exchange. A proposal for a new Transparency Regulation has recently been issued by the Commission.

Finally the Environmental Information Directive 2003/4/EC seeks to guarantee to the public the right of access to ‘environmental information’ held by or for public authorities. Certain of
the data described in this Study could be classified as environmental information. Requests for such information may only be refused on narrowly defined grounds specified in the directive which must be interpreted in a restrictive way.

7 Conclusions

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.

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.

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.

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. Alternatively, any proposed data sharing mechanism would need to ensure that recipients of the data are equally bound by confidentiality.

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.

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.

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.

---

4 In this connection it is to be noted that the Control Regulation is currently being revised.
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).

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.

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.

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.

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).

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.

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?
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.

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.

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.

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.

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.