LEGAL WORKING GROUP (LWG)

FINAL REPORT ON BLUEMASSMED
LEGAL ISSUES

July 2012 *(V.26.07.2012_PT)*

*"**Great is the reign of the Sea**"*

Thucydides,
Histories, Book A, verse 143.

INDEX

1. INTRODUCTION

In the scope of maritime surveillance strengthen of the cooperation between the different countries is an important goal to achieve. The United Nations Convention on the Law of the Sea, also called the Law of the Sea Convention, already defines the rights and responsibilities of nations in their use of the world's oceans, establishing guidelines for the environment, and the management of marine natural resources.

In consideration of those priorities set by the European Union about sustainable development in the maritime sector[1] on maritime security and safety[2], maritime monitoring and surveillance data was gathered within and around European waters by a range of agencies for a number of different purposes[3].

Communications of the European Commission and Conclusions of the Council were adopted[4], setting out its vision for an Integrated Maritime Policy for the EU, whilst at the same time outlining a working program for the years ahead.

The BMM pilot project that runs, in parallel, in the Mediterranean basin, to test in the theatre of operations how integrating maritime surveillance can work in practice, is one of the steps towards the regional integration of the European maritime reporting and surveillance. This goes beyond border related aspects, thus covering all maritime activities, such as maritime safety, protection of the marine environment, fisheries control, law enforcement, border control and defense, as it is envisaged by the CISE framework.

The Legal Working Group (LWG) was entitled to identify what possible legal obstacles may exist to the sharing of maritime data between the different authorities/agencies and the possible solutions taking already into account the rules of the Lisbon Treaty and the relevant rules of each MS. In order to achieve

[1] Parallel to the respective legislation of international instruments (IMO) .
[2] Convention SOLAS, Chapter XI – 2, ISPS Code.
[3] Directive 2002/59/CE.
[4] Validated by the Council through its conclusions on the 3092nd General Affairs Meeting in Brussels, on the 23 May 2011..

the knowledge of sufficient information from the parties to comply with the project, the LWG performed a legal questionnaire that merged the specific data from each country. This consolidation contributed to a very relevant state of play of the legal obstacles regarding the data exchange in the scope of the maritime situation information.

Also, the need of doing something practical in order to support the demonstration phase resulted in the elaboration of a Legal Manual.

Moreover, the LWG prepared a list of EU and international legislation documents related to data exchange, submitted on the present report.

2. OBJECTIVES AND ACHIEVEMENTS

The main aim behind this pilot project that runs in the Mediterranean basin is intended to test, in the theatre of operations, as to how to effectively integrate maritime surveillance, this in itself being one of the major steps towards the regional integration of the European maritime reporting and surveillance. In other words, this project goes beyond border related aspects, thus covering all maritime activities as it is envisaged by the CISE framework.

Undoubtedly, the exchange of information is an indispensable tool in the accomplishment of the missions by all parties involved, particularly when, on account of all existing systems and respective competences, the overriding goal will be that of creating some form of synergy between the parties that will ultimately attain far better results, in terms of cost, effectiveness and efficiency.[5]

At the same time, the delivery, in real time, of data and intelligence is fundamental for the parties in order to prevent and detect maritime incidents with success, in accordance with their competences, having in mind that European Union has common borders. Indeed, one of the objectives of the

[5] The added value in integrating maritime surveillance is to **enhance the present sectoral maritime awareness pictures of the sectoral User Communities of EU Member States and EEAStates with additional relevant cross-sectoral and cross-border surveillance data on a "need to know" and a "responsibility to share" basis. The requirement to share information, particularly in case of an imminent threat, should be balanced by its owner against the risk of not sharing it.** Such enhanced pictures will increase the efficiency of Member States' authorities and improve cost effectiveness. *Vide* GP2-CISE Step 4.

Integrated Maritime Policy for UE is to overcome complex legal issues such as data protection and ownership. For this reason, the parties need to identify the legal provisions that must be complied with in order to enable a lawful exchange of maritime surveillance data.

It is important to apply the legal framework, taking due consideration of the legal constraints, yet defining rules that permit the parties to exchange information.

The BMM's legal purpose is that of providing a pronounced fieldwork insight into the legal issues and solutions encountered by the parties and the ways how to resolve them.

A clear legal framework need to be established, defining at least the nature of the data involved, the capability of the data providers, the purposes (and the methods) of the exchange and the potential recipients of the data. The necessary safeguards with regard to the confidentiality and security of data and the protection of personal data need to be respected by the recipient of the data.

The summary report on the *"Legal aspects of maritime monitoring & surveillance data Summary report"*, as of October 2008, done for and on behalf of the European Commission, examined the potential legal barriers to the exchange of maritime monitoring and surveillance data primarily on the basis of International and European Community (EC) law.

Based on that legal study and taking into account the entry into force of the Lisbon Treaty, on 1 December 2009[6], and the work of the BMM Legal Working Group through consultation with BMM parties and other non-participating BMM entities, there emerged the need in coming up with something practical in order to support the demo phase of this project.

Thus, the Legal Manual is the "operational" end result following the identification of possible hurdles and obstacles brought to the fore each BMM Member State (MS) up to European level.

3. WORKING METHOD OF LWG

[6] TFUE, articles 326 – 334.

Regular meetings were organized in different places at different stages of the project;

Dedicated website (http://www.bluemassmed.net/) with private work space, exchange documents and ideas between BMM MS and to work at expert level, for example definition of sensitive and intelligence data;

Synchronization with Users Working Group (UWG) and Technical Working Group (TWG):

- Identification of the data to be exchanged by the UWG;

- Elaboration of the systems of data exchange by the TWG;

- Analyses and evaluation of the issues on the two previous sentences;

- Reaching a common legal point of view between BMM MS;

- Communicate with national and European data protection authorities about experimental demonstration;

- Taking into account the point of view of all participants MS agencies and European agencies and industry and environmental stakeholders;

- Identify significant obstacles and propose recommendations to improve the overall legal framework.

4. DATA EXCHANGE BETWEEN BMM MEMBER STATES

In this specific approach, the main objective of this consolidation is to underline and reveal the general perspectives and the specifications of each country regarding the most relevant aspects having also into account the significant regimes, systems and mechanisms.

E.g. Questionnaires in the Annex.

4.1 REPORTING REGIMES

Under this scope are included those regimes whereby data must be actively reported by a person or vessel subject to the applicable regime.

- Data from **Automatic Identification System (AIS)** can be made available with no restrictions;
- **Long-Range Identification and Tracking of Ships (LRIT)** data is not shared because contracting states receive the information, but they can´t exchange with another states, it is effectively a closed system. LRIT is not yet fully operational;
- **Vessel Monitoring System (VMS)** data received is confidential information that is exchanged between the competent authorities of the coastal and the flag state.

4.2 SURVEILLANCE SYSTEMS

Under this scope, 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, as:

- **Vessel Traffic Services (VTS)**: There are two basic types of VTS – coastal and port. 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 information received from VTS is made available of on a selective and secure basis;
- **Military Surveillance Systems:** The gathering of surveillance data is inherent to the role of Europe's navies for defense purposes, which since 2001, includes defense against terrorism;
- **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 commercial satellite providers according to action planned with MS.

- **Sistema Integrado de Vigilancia Exterior (SIVE**) : Operated by the Spanish Guardia Civil is a Coastal surveillance system that is based on a network of fixed stations and mobile units that make use of still cameras, CCTV, radar and infra-red sensors.
- **SIVIIC** – Operated by the Portuguese National Republican Guard, is an Integrated Surveillance System.

4.3 DATA SHARING MECHANISMS

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 stockholders. They provide for the sharing of maritime surveillance data both internationally and within individual Member States, as:

- **SPATIONAV** – National data sharing mechanism: designed to collect and compile data generated by a range of sensors to assist maritime operational centers. France information is managed by the navy which is connected to Traffic 2000 and SafeSeaNet.
- **Regional AIS** : The HELCOM AIS Network enables the real time sharing of AIS data among the parties to 1992 Helsinki Convention ;
- **SafeSeaNet** : is a data exchange system developed by EMSA to support the implementation of elements of the VTM Directive ;
- **Commercial AIS** : AIS Live is owned by Lloyds Register Fairplay Limited and the acess to the service is by subscription ;
- **Virtual Maritime Traffic Centre (V-RMTC)** : Virtual network connecting the operational centres of number of navies that enables the sharing via internet of unclassified information on merchant shipping ; Coordinated by the Italian Navy.

4.4 CATEGORIES OF DATA

Different categories of information were identified regarding basic data, additional data and restricted data[7], meaning that:

- Basic data are free to exchange with no legal constraints, although it's important to be aware that, for instance, information regarding ship owner and ship company, as well as ship photograph, may be considered personal data if permit the identification of a natural person;
- Additional data are accessible from certain selected sources although it's subject to generic legal conditions for exchange (e.g. purpose related, or subject to third party licensing, etc). Usually referenced as case by case analysis;
- Restricted data, the ones which availability is restricted by law.

4.4.1 Personal Criminal Data

In order to enable the users to the concept simple, the following formulation was choosed: Personal data are deemed criminal, those contained in criminal records of MS, as well as those who alone or combined with other identifying a person and are already integrated in ongoing criminal proceedings.

Access to personal data of a criminal nature are generally subject to authorization by the competent judicial authority, observing the principles of legality, protection of private life, broad sense of proportionality and human dignity, and may still have access to this data *ad conditio*, in addition to the shares of procedure, only the criminal police and the criminal police authorities (*under national laws of criminal procedure*).

In most MS exchange of criminal information of personal data is always carried out by authorization of the competent judicial authorities, when such data already incorporate a criminal proceeding, or done by the criminal police bodies while still not part of the process- crime, dealing in this case the mere exchange of information within police oriented proactive police subordinate to the principle of legality and proportionality broad sense and without prejudice to

[7] E.g. Legal Questionnaire and Matrix in the Annex

subsequent supervision of judicial authorities if such data is liable to be used in future criminal proceedings.

Thus, in accordance with treaties and international and European judiciary cooperation in criminal matters, the Judicial Authority and the criminal police are unable, in the light of the case (case-by-case basis), to make exchange of personal data criminal, with other agencies to whom the MS law assigns equal competencies.

Therefore in terms of exchange of information and personal data handling criminal, judicial authorities and the police do not share information with those to whom the internal law of MS does not give equal powers.

The EU Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the MS' of the EU that has already been transposed into national law of each MS establishes that law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.

Having into account preamble (3) of this Framework Decision "*exchange of information and intelligence on crime and criminal activities is the basis for law enforcement cooperation in the Union serving the overall objective of improving the safety of the Union's citizens*."

Indeed, preamble (5) sets that "*it is important that the possibilities for law enforcement authorities to obtain information and intelligence concerning serious crime and terrorist acts from other Member States be viewed horizontally and not in terms of differences with regard to type of crime or division of competencies between law enforcement or judicial authorities*."

The article 1 nr.1 gives an overview of its application to existing information and intelligence inside criminal investigations or criminal intelligence operations and article 3 nr 2. establishes that information and intelligence shall be provided at the request of a competent law enforcement authority and article 3 nr 3. that "*Member States shall ensure that conditions not stricter than those applicable at national level for providing and requesting information and intelligence are applied for providing information and intelligence to competent law enforcement authorities of other Member States*."

Article 7 nr 1. sets that "*the competent law enforcement authorities shall, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA (European arrest warrant).*"

In conclusion, law enforcement authorities shall share criminal data and intelligence at the request of a competent law enforcement authority.

If there are reasonable reasons to believe that it will contribute to detection, prevention or investigation on specific crimes, the entities that are not law enforcement authorities may receive criminal data and intelligence on a case-by-case basis (need to know principle).

The ones that are not law enforcement authorities receive criminal data and intelligence on a case-by-case basis and based on the principle of legality and proportionality broad sense (need to know principle) if there are reasonable reasons to believe that it will contribute to detection, prevention or investigation on specific crimes.

Outside EU members IAW Article 6 nr 2. (Council Framework Decision 2006/960/JHA, of 18 December 2006) – "*Information or intelligence shall also be exchanged with Europol ... and with Eurojust ... with a view to reinforcing the fight against serious crime*".

Article 3 nr 5. sets that where the information or intelligence sought has been obtained from another Member State or from a third country and is subject to the rule of specialty, its transmission to the competent law enforcement authority of another Member State may only take place with the consent of the Member State or third country that provided the information or intelligence.

Other legal instruments related to information exchange for the purpose of criminal investigations and criminal intelligence must be taken into account, such as: Convention Implementing the Schengen Agreement of 14 June 1985 and all related legal instruments; Convention on the use of Information Technology for Customs purposes (CIS Convention); Convention on Mutual Assistance Cooperation between Customs Administrations (Naples II Convention); Council Regulation 515/97 and Council Regulation 766/2009

amending Regulation 515/97; Prum Decision (Council Decision 2008/615/JHA of June 2008 on the stepping up of cross border cooperation); Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; geographic information such as maps, geographic coordinates and geo data should be in line with directive 2007/2/EC of the European Parliament and of the Council of the 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

Those legal instruments already provide specific rules to facilitate the collection of and sharing information between national authorities and other European “players”.

For example, Portugal can share this data between all law enforcement authorities on a case-by-case basis due to restrictions that exists on the sharing of data pursuant to data protection law. When it comes to criminal data, the Portuguese act nr 74/2009, of 12th August, transposed the EU Council Framework Decision 2006/960/JHA.

However, Portugal is also an established legal regime applicable to the processing of data relating to the judicial system, with relevance to the exchange of personal data between the judiciary and various entities policed MS, this regime is enshrined in Law 34 / 2009 July 14, and among various purposes that this law intends to regulate stands out with relevance to the BMM project, the purpose of ensuring the completion of investigation and prosecution, under the Constitution and laws, as well as compliance with the laws of criminal policy, compliance with the judicial authorities of the obligations arising from international judicial cooperation law and the instruments of international law and European Union, to provide criminal police organs of the data necessary to fulfill the obligations of data exchange and information to fight crime and preserve the law and the emerging international legal instruments and the European Union and ensure the execution of arrest warrants national, European and international.

In the French case, these data are collected by national data-basis previously authorized by the French data protection authority (DPA), in accordance to the law protecting personal data.

4.4.2 Criminal Personal Intelligence

4.4.2.1 General Data

In particular personal intelligence is the collection of criminal data via secret information tends to be acquired or less public and police activities exclusively in pro-active in the pure crime prevention, prevention in the fight against organized crime or crime of mass[8] .

This type of information within the designated criminal intelligence, is generally performed by collecting information provided by ordinary citizens, whether through the medium (public sources) and by collecting and processing information, often generated by the agents of the police interrogation, inquiries, observations, interviews, information received through other people or even the mere rumor of research (human intelligence) and also the designated technical intelligence collected by a variety of technological means, such as means of locating and monitoring of radio, radar and other similar devices, communications intelligence, electronics, telematics and exploitation of computer networks, etc[9].

In terms of internal orientation of each MS, we must consider the following restrictions and permissions for data gathering criminal intelligence personnel.

In France, general data and information's are collected by national law enforcement authorities (police and customs in France) before the stage of criminal investigations. Data intelligence could be shared between by French law enforcement authorities on a case by case basis.

In Portugal, when it comes to Personal information (criminal) such as incidents and violations including those placed on black/grey lists, ships involved in maritime events including events involving their cargo or crew/owners, the same legal framework as "Criminal personal data" is applied. In legal terms, the personal criminal intelligence is not required by the law of criminal procedure. The criminal procedure law limits the actions of the police

[8] (as was defined by Professor Winfried Hassemer, in "The Public Safety rule of law, Associaçâo Academica da Faculdad de Direito de Lisboa, 1995, p. 91)

[9] Italy disagrees with the paragraph, because according to Italy, such activities are out of the scope of the BMM Project and are conducted in accordance with the European and National legislation.

intelligence collection and treatment indication and urgent investigation and precautionary time limited. However, it is permissible to combat serious and organized crime using special methods of investigation for purposes of crime prevention and investigation criminal pro-active, such as covert operations, but only with permission of the judicial authority, namely the trial judge when it comes to pure crime prevention activities, or the competent prosecutor Public, mandatory reporting by the Magistrate, in the case of covert investigations under the criminal proceedings already in progress and always in control of the judicial police (IAW Portuguese Law 101/2001, of August 25).

4.4.2.2 Information regarding incidents and violations, including those placed on black/grey lists

This kind of information could be shared on the case by case basis between law enforcement authorities.

4.4.3 Data that depends on the authorization of the competent judicial authority

MS can only share this data with the authorization of the judicial authority, having into account the provisions of article 3 nr 4 of the Council Framework Decision 2006/960/JHA: *"Where the information or intelligence sought may, under the national law of the requested Member State, be accessed by the requested competent law enforcement authority only pursuant to an agreement or authorization of a judicial authority, the requested competent law enforcement authority shall be obliged to ask the competent judicial authority for an agreement or authorization to access and exchange the information sought."*

4.4.4 Personal Data (Not Criminal)

The main common issue is the processing and handling of personal data, whose definition is established in article 2 of Data Protection Directive, Directive 95/46/EC, of 24 October 1995, on the protection of personal data and on the free movement of such data. So, "personal data" shall mean "*any information relating to an identified or identifiable natural person ('data subject'); 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*".

Article 6 of Data Protection Directive sets principles related to data quality: the data must be processed fairly and lawfully; data may only be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes; data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed and the data has to be accurate and necessary and also kept up to date.

Article 7 sets principles related to the legitimacy of data processing. This shall mean "*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*".

This is always having in mind that there's a controller which shall mean "*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 processing are determined by laws or regulations, the controller shall be designated in the Act establishing the organization and functioning or in the statutes of the legal or statutory body competent to process the personal data concerned*".

Moreover, having into account that the recipients the natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

In France, data are allowed to be shared in accordance to "*informatique et libertés*" law of 2004 which has transposed the 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 processing of data must be permitted by the French data protection authority ("*CNIL, commission nationale informatique et libertés"*).

However, we have to pay attention to the commercial data which could be collected through shipping companies' information. Indeed, the commercial and industrial secret is protected by the French intellectual property code ("*code de la propriété intellectuelle"*).

Some companies sell data coming from Automatic Identification System (AIS). Indeed, this one is an open source system; so, all kinds of people can intercept the information sent by AIS with only a VHS. For some of those companies, the data of the AIS would not be protected. That's why they can sell them.

Another debate is in relation to the restrictions in the contracts with data providers who impose their data protection policy. Such agreements lead to restrictions in the communication of data provided. Thus, "bilateral shipping agreement information" of Lloyd's register fairplay Ltd, provides that "*the client accepts the confidentiality of the data and shall not disclose the contents of the services under any circumstances and in any form to a third party* ". Consumers, like public authorities, are obliged not to share the information received when they are not into the public domain.

However, the validity of such confidentiality clauses may be questioned. The commercial exploitation of the data of the AIS is not admitted by the IMO. The latter has condemned these practices on the 79th assignment of the Committee on maritime security held in December 2004, in the following terms: the maritime security Committee "*condemned the regrettable publication on the world-wide web or elsewhere of AIS data transmitted by ships; condemned those who irresponsibly publish AIS data transmitted by ships on the world-wide web or elsewhere, particularly if these offer other services to the shipping and port industries; and requested the Secretary-General to bring to the attention of those who publish or who may publish AIS data transmitted by ships on the*

world-wide web or elsewhere, the conclusions of the Committee. This statement remains political, was carrying no practical effect because of the impossibility for the IMO to sanctions in destination companies under private law. Therefore, how intends a society to assert his rights on illicit information? This explains that in practice, these companies do little of the use of the information concerned".

In Portugal, general data can be shared respecting the legal restriction of data protection law. IAW the conditions of Act 67/98, 26th OCT that transposed Directive 95/46/CE - on the protection of personal data – an authorization of DPNC must be acquired.

The exchange of information outside EU IAW art. 19, nr 1 of Act 67/98, of 26 October and art. 25 of Directive 95/46/CE, "*may only take place subject to compliance with this Act and provided the State to which they are transferred ensures an adequate level of protection*".

Regarding information about shipping companies (e.g. commercial operator; registered owner; crew list) there are two possible problems:

- Sometimes there are contractual confidentiality that doesn't permit to share information and
- If the information contains personal data an authorization of National Data Protection Authorities have to be follow.

4.4.5 Another kind of data related to surveillance information

Related to information about vessels (e.g. ship identity, current voyage data, imagery of the ship and cargo information including risk classification) **s**ometimes there are contractual confidentiality that doesn't allow sharing information.

Information about national maritime assets that contribute to maritime surveillance (e.g. deployment schedules; routine patrol areas) is data shared on a case-by-case basis because it's classified information.

Regarding information about national maritime areas of focus (e.g. exclusion zones, sea routes) and information about land-based national maritime surveillance sensors (e.g. positional information) only the information available in open sources is shared.

Information from national maritime ports (e.g. cargo information; running list of vessels scheduled in port and at anchor; historical data) sometimes is not all available in web open sources; Furthermore, it is possible to have contractual confidentiality that doesn't allow to share information.

5. REFERENCE TO DEMONSTRATION

For the Demonstration there was prepared a legal manual by the Legal Working Group in order to be used by the Users of BMM. That manual was containing guidelines, recommendations and best practices. To the extent that manual touched upon matters related to data protection.

A communication with national data protection authorities was made about the experimental demonstration.

6. SUMMARY OF IDENTIFIED POTENTIAL LEGAL RESTRICTIONS

The purpose behind the sharing of data shall be a fundamental pre-requisite to any data sharing mechanism. A clear and precise description of the purposes behind the data exchange mechanism is therefore of crucial importance (e.g. illegal trafficking and immigration) in the same manner as the respect of the legality and proportionality principles.

6.1 Personal Data

Personal data is not to be processed for purposes other than those for which they were collected.

Specifically in relation to the sharing of personal data, purpose-limitation and proportionality are fundamental principles which need to be taken into account.

Processing of personal data is an "identified" potential restriction on data sharing the name of a vessel is not sufficient to directly identify a (natural) person owning a vessel.

However, 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, analyzing maritime surveillance data we can conclude that some data involve personal data (e.g. where data concerns a fishing vessel identification number, a license 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 majority of cases the owner or agent of a vessel will be a legal person this may not always necessarily be the case.

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. [10]

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

Transfer of personal data outside the European Union (e.g. INTERPOL) *"may only take place subject to compliance with Data Protection Law and provided the State to which they are transferred ensures an adequate level of protection"*[11].

[10] *Summary Report*, 2008, page 10.

[11] IAW article 19 of Portuguese Act 67/98 of 26 October Act on the Protection of Personal Data (transposing into the Portuguese legal system 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).

It should be clear in the matrix that some data are not exchangeable for contractualized and it is up to each Member State to take the responsibility to engage with the companies in question through public-private agreements, as did the EU (see the National Plan to Achieve MDA). This issue will come back on the mat at one time or another, especially if the EU continues its efforts to become a member of the IMO and not just observers.

6.2 Confidentiality and commercial/professional secrecy

Confidentiality can be originated:

a. Through legislation due to the inclusion of express legal provisions to this effect, or
b. On the basis of contractual provisions as page 20 of the Demonstration Executive Plan 1.3.

While certain legal provisions are not to debar, as such, the exchange of data, recipients of such data are duty bound not to disclose it to third parties not specifically mentioned within the relevant legal framework (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 the "duty of confidentiality" on users and effectively prohibits unauthorized third party re-use). Similar provisions emanate from the end user licence for CleanSeaNet, including a purpose limitation, the effect of which is the MS may use the data solely for the purpose of oil spill monitoring.[12]

A significant amount of surveillance data is qualified and/or has to be treated as (commercially) confidential. As a consequence, the processing of this data will be affected by the duty of confidentiality and professional secrecy of the persons authorized to have access to the data.

With regard to the use (including the sharing) of maritime data, sectorial 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). Additionally, it should be taken into account that, if the sourcing of sharing of

---

[12] *Summary Report*, 2008, pages 9, 10.

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).[13]

6.3 "Confidence Classification"

"Confidence Classification" (deriving from the statistical measure of reliability of results), as used in BMM is divided into:

1 - Very high confidence, verified data;
2 - High confidence (cooperative/ non cooperative correlation);
3 - Confidence (non cooperation/ non cooperation correlation or coop/ coop correlation);
4 - Low confidence (unsure source of verification, low confidence correlation);
5 - Very low confidence (no verification, co-operative target TBC).

Thus this terminology (CONFIDENCE) should not be misunderstood as belonging to the definitions given in the previous paragraph (CONFIDENTIALITY).

7. OTHER ISSUES TO CONSIDER

7.1 PARTICIPANT'S RIGHT OF ACCESS

Legal framework of data protection define "recipient" as a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party is involved or not. However, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.

[13] *Summary Report*, 2008, page 14.

The right of access by users to the BMM data was one of the most important aspects of the project. Individual access to BMM data by users was made upon “the need to know principle”, and according to a confidential classification it was specially elaborated for the BMM project.

Regarding to “the need to share principle”, involved by the Commission, it is necessary to keep in mind some legal aspects. A median possibility is to take into account, using the notion of “responsibility to share” instead the concept of “need to share”. For example, the objective to share data between customs authorities and police agencies was made possible, during the demonstration.

7.2 PERSONS RIGHTS

The controller of the processing of BMM systems has to be in line with existing EU and MS legislation, following rights deriving from MS legislation are guaranteed:

- Right to information of the subject;
- Right of access of the subject, directly or indirectly, according to national legislation;
- And finally Right to provisional judiciary protection of the subject;
- There is no right to opposition of the subject.

7.3 DATA SECURITY POLICY

In order to protect BMM data during the demonstrative phase the contractor has adopted the necessary security in order to:

a. physically protect data;
b. deny unauthorized persons access to national installations in which the Member State store data (checks at entrance to the installation);
c. prevent the unauthorized reading, copying, modification or removal of data media (data media control);

d. prevent the unauthorized inspection, modification or deletion of stored personal data (storage control);
e. prevent the unauthorized processing of data (control of data processing);
f. ensure that persons authorized to access the data have access only to the data covered by their access authorization, by means of individual and unique user identities and confidential access modes only (data access control);
g. ensure that all competent authorities with a right to access the data create profiles describing the functions and responsibilities of persons who are authorized to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities without delay upon their request (personnel profiles);
h. ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
i. prevent the unauthorized reading and copying of personal data during their transmission, in particular by means of appropriate common protocols and encryption standards (transport control).

7.4 ACCESS TO PUBLIC SECTOR DOCUMENTS

At EC level the principal instrument is the Transparency Regulation (EC) 1049/2001 which regulates public access to documents held by Community institutions. This document seeks to balance the main principle that all documents should be accessible to the public, in spite that in some circumstances certain public and private interests are protected as an exception to this rule. MS 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 surveillance data were to be so classified this might constitute a barrier to their exchange.

7.5 REMOVING OBSTACLES TO DATA EXCHANGE

Every Member State when building data exchange models shall comply with data protection legislation at EU level and at national level (for BMM Member States).

7.5.1 Common use of military and civil data

Civil and military data fusion was a success during the BMM experimentation. For the first time defense data of military nature were made available to civilian users and vice versa. For example, SPATIONAV systems (military data), used in France to establish a single real maritime picture, could be enriched with additional civil from customs authorities.

In a legal point of view, it can be considered as a new domain in the European area since the Lisbon treaty. For instance, data protection law is not applicable in all MS for military entities. These questions will be part of the discussion on the new data protection framework in Brussels (DAPIX) and was already approached in some discussion about “Piracy” in the European parliament.

7.5.2 Private commercial data right questions

It appears that some companies sell data coming from AIS. Indeed, this is an open source system. As a result, all kind of people can catch the information sent by AIS with only a VHS. For some of those companies, the data of the AIS would not be protected. That is why they can sell them. Another debate is in relation to the restrictions in the contracts with data providers who impose their data protection policy. Such agreements lead to restrictions in the communication of data provided. Thus, “bilateral shipping agreement information” of Lloyds register fairplay Ltd, provides that “client accepts the confidentiality of the data and shall not disclose the contents of the services under any circumstances and in any form to a third party”. For instance, consumers, as public authorities, must not have the information received when it is not the public domain.

7.5.3 Maritime data on maritime safety and intellectual property law

7.5.3.1 The AIS data in open source

The EC adopted a directive on monitoring traffic that carries maritime serious consequences on the free availability of data collected via the different technologies used. Thus, Article 24 of that directive states: "*the States shall take the necessary steps in accordance with their legislation national, to ensure the confidentiality of information transmitted to the under this Directive*."

AIS data received as part of the Community must, therefore, be protected. However, the Community felt that this protection was in no way an obstacle to exchange them between Member States and the Commission. These data are public, and about what mode acquisition and processing, legislation concerning the right property intellectual can not apply.

Another debate surrounds the AIS and it was initiated by providers' market data. For some, the data from the AIS, by their lack of protection, would not be protected. This discussion is coupled with another debate related to restrictions encountered in connection with contracts with data providers who impose their policy Protection information. Such agreements invariably lead restrictions in the communication of data. Thus, the "bilateral shipping information agreement "Lloyd's Register Fairplay Ltd", provides that "the customer accepts the privacy and should not disclose the contents of services under any circumstances and in any form to any third party." The consumers, such as public authorities are bound by confidentiality information received when they have not fallen into the public domain.

However, the validity of such confidentiality clauses can be challenged case, the commercial exploitation of AIS data is not accepted by the IMO.

The latter, indeed, condemned these practices on the occasion of the 79th transfer the Maritime Safety Committee held in December 2004, in following terms: "*The Maritime Safety Committee condemned the regrettable publication on the web or by other means, of AIS data and condemns those who have irresponsibly published or decoded data transmitted by ships, particularly where this has implications for providing services 11 Directive 2002/59/EC of 27 June*

2002 on the establishment of a Community monitoring of vessel traffic and information. to shipping lines and port industries." This statement remains a political, not taking any practical effect because of the inability of IMO to impose sanctions destined for private law firms.

Consequently, how a company intends to pursue their claims on information Illegal? This explains, in practice, these companies do not care much for the use made of the information.

7.5.3.2 The public-private agreements

Partnerships with private companies are one of the orientations of the United States in the development of their MDA (Maritime Domain Awareness). The National Plan to Achieve MDA insists that such partnerships are needed to ensure full control of the domain maritime. The public-private agreement between customs and past societies commercial against terrorism provides a model for improving and encourage private sector participation. Especially since the Coast Guard Americans have this condition imposed on each company wishing to gain ports U.S..

Such collaborations can be extremely profitable because companies are causing the flow of goods and have, therefore, information of the first order on the contents of vessels bound for ports.

It seems that the intervention of private actors in the exchange of information related maritime safety, whether at Community level with BLUEMASSMED, or in terms of NATO with the MSA, is difficult to implement. The real question is whether it is really possible, regardless of the constraints legal, to do without the participation of private operators. The United States seem to have brought a part of the answer by choosing to cooperate and exchange with private companies.

In the event that the European Union would engage in this logic, it would first consult with IMO in order to remove all barriers to the transmission of data by private actors. This choice is no longer legal but political.

7.5.4 Lisbon Treaty

Lisbon Treaty and cooperation mechanism for cooperation.

Sections 326 to 334 TFEU specify the mode of application of Article 20 TEU on enhanced cooperation.

1) Requirements.

The Treaties and the Union law must be respected and enhanced cooperation:

- Can not address an area of exclusive competence of the Union;

- May not affect either the internal market or economic, social and territorial

- Can not constitute a barrier to or discrimination in trade between Member States, nor shall it distort competition between them;

- Can be launched as a last resort that is to say where it is established that the objectives can be attained within a reasonable period by the Union as a whole (Article 20 TEU).

The threshold for enhanced cooperation is to New Member States (a third of the States of the Union) and well organized cooperation must remain open to all Member States.

2) The authorization procedure.

Permission to trigger enhanced cooperation shall be granted by the Council, acting by qualified majority on a proposal from the Commission (presented at the request of States concerned) and after approval of the European Parliament (whose members may be taken by vote or not they were elected in the Member States concerned).

Within the areas of sections 82, 83, 86 and 87 TFEU (judicial cooperation in criminal matters, definition of criminal offenses and penalties relating to terrorism, human trafficking, sexual exploitation of women and children, drug trafficking and weapons, money laundering, corruption, counterfeiting of means of payment, computer crime and organized crime, measures to fight against the financial interests of the Union, police and customs cooperation for the

prevention, detection and investigation of criminal offenses, which also involves the collection, storage, analysis and exchange of relevant information), an "acceleration clause" was intended.

Description of the "acceleration clause" in the areas mentioned above: if, during the procedure for adopting Community legislation in these areas, unanimity is not reached within the Council, a group composed of nine Member States may request that the European Council itself know of the draft act. In case of consensus, the European Council has four months to return the draft to Council for adoption. In case of disagreement within the European Council, and at least nine Member States wish to establish enhanced cooperation on the basis of the draft act under discussion, they shall inform the European Parliament, Council and Commission. In this case, they are allowed to proceed with enhanced cooperation between themselves, on the basis of that act.

Whatever the procedure used, expenditure other than administrative costs are borne by the participating Member States, unless the Council decides otherwise, shall unanimously and after consulting the European Parliament.

3) The "gateway" to move from unanimity to qualified majority and the special legislative procedure to the ordinary legislative procedure.

According to Article 333 TFEU, when, as part of enhanced cooperation, a provision of the TFEU provides for unanimity, the Council may, unanimously predict that it will act by qualified majority. It's the same with regard to the passage of the special legislative procedure to the ordinary legislative procedure.

4) The case of the CFSP.

On CFSP enhanced cooperation can be triggered only by permission of Council acting unanimously, on request of States concerned, the Commission giving notice and being not only informed the Parliament. The High Representative also gives its opinion.

The gateway is applicable, except for decisions with military implications or in the field of defense.

Finally, with regard to European defense, a simplified procedure for cooperation is provided through three schemes:

- Permanent structured cooperation (Articles 42 and 46 § 6 of the TEU and the Protocol to the Treaty of Lisbon) for Member States with military capability is high and which have made them more binding commitments in this matter;

- The participation of a group of Member States to Mission CFSP (maintain peace, humanitarian, evacuation etc.; Article 44 TEU);

- The European Defence Agency, which is open to Member States wishing to participate to enhance their military capability (Articles 42 § 3 and 45 TEU).

8. OVERALL CONCLUSIONS

In the context of BMM pilot project, the LWG was tasked to identify the legal barriers to data exchange, maritime and personal, between the different authorities or agencies of the MS and propose legal recommendations to overcome those conflicts.

Since the beginning it was clear for the LWG that the most relevant legal issues were related to personal data and confidentiality. An unavoidable amount of maritime reporting and surveillance data is qualified, in the national legal framework of MS, as confidential. The importance of addressing these questions properly, giving them the importance that they claim, clearly became the main concern of the LWG work.

The entire block of legal dispositions which focuses on information exchange and personal data was taken into account. The LWG also considered the statutory provisions contained in the Lisbon Treaty, the constitutional texts and principles of the several MS, the relevant European legislation and provisions (regulations/directives/framework decisions) and also the UN Convention on the Law of the Sea (Montego Bay Convention), as well as several International Agreements.

The LWG soon identified the main obstacles to its study and analysis. The path for their removal had to be followed and clearly became the only way to guarantee the inherent process of research.

First, the legal mechanisms concerning to data protection (criminal and non criminal) differ from state to state and this fact becomes an obvious barrier to achieve the desired standardization and consolidation of sharing procedures, notwithstanding the existence of Directive 95/46/EC Parliament and Council of 24 October 1995. LWG goal was to identify a common pool of legal constraints to obtain a common global picture of prohibitions and possibilities, meaning, to obtain the specific legal context of data sharing.

Another legal obstacle that the LWG had to deal with was the extent and opacity of the core of fundamental rights within the national constitutional provisions. It was not always easy to reach a consensus regarding the possibility of compression or limitation of important legal and constitutional principles as the principles of legality, proportionality and right to privacy, among others.

Controlling and monitoring the maritime area of the EU is an absolute challenge for the MS. It is a common space constantly exposed to illegal and criminal activities, implying a synergistic effort to ensure common security and social peace within it. For this reason it is extremely important the need to ensure collaboration among various MS agencies, in an equally synergistic manner, in order to put in place an appropriate legal framework that addresses the most relevant legal issues concerning the interconnection of data systems.

The main purpose of this LWG was to identify the nature of the data shared by the surveillance mechanisms involved and then to edify a frame of identified potential legal restrictions, concerning to personal data, professional/commercial secrecy, participants and persons right of access, data security policy and access to public sector documents.

The LWG identified that the purpose behind the sharing of data is a fundamental pre-requisite of any data sharing mechanism. Therefore, the purposes must be clearly and precisely described (illegal trafficking, immigration, etc.).

It is also necessary for the MS to identify the entities and agencies with responsibilities of law enforcement in the maritime environment that are able to carry and promote the inter-state exchange of information.

Moreover, personal data (natural or legal person) or commercial data, inserted in criminal proceedings which are still in trial procedures, therefore, not

final, can not be exchanged between the MS without permission of the competent judicial authority.

Beyond these cases, the LWG believes there are no legal restrictions on the exchange of personal data between law enforcement authorities of the MS, if made for purposes of criminal prevention (as set in EU Council Framework Decision 2006/960/JHA – Swedish Decision), safeguarding the rights of nationals and residents, as well as commercial rights, under the consent of the responsible data protection authorities.

To sum up, the LWG concluded that despite of the existing and identified legal constraints concerning to data use (and sharing), it is possible to create an actual practice of exchanging information in a timely manner, so as to enable prevention and suppression of illicit activity. To do so, it is mandatory that trust be the basis of the relationships between all partner agencies in all MS.

9. BMM LWG FINAL STATEMENTS

a. There are no legal obstacles in the exchange of data within the Member States regime. Every kind of contribution of basic data (demonstration) is included, as well as sensitive data (police – customs) empowered by the Swedish initiative (EU Council Framework Decision 2006/960/JHA).

b. A communication to the National Data Protection Authorities is needed (data security policy- individual/ fundamental rights) in order to enable MS to exchange data within the scope of maritime surveillance.

c. The BMM pilot-project was successful in the fusion of basic civil-military data and vice-versa, meaning that it reinforced the already existing military use of civil data, as well as it provided the use of military data for civil purposes.

d. The continuation of the function initiated by the BMM after the end of the pilot-project's period have to consider the legal restrictions imposed by the Lisbon Treaty within the scope of reinforced cooperation (indeed 9 MS are required; only 6 Member States available within BMM). An European framework

would be necessary to go on with the existing BMM Communities on a potential cross-sectorial/ cross- border aspect.

e. Issues of intellectual property rights of public entities are out of question within the BMM pilot project, as well as in the scope of maritime surveillance. However, issues regarding the property on commercial data deriving from the private sector may have to be considered under a different approach, namely endeavour the possibility of a mixed public-private agreement (e.g. USA precedent).

f. “Need to know” principle in balance with “responsibility to share” principle leads to a paradigm shift on behalf of the user’s communities towards an increasing common trust and awareness of the “interest to share” and its added value.

10. RECOMMENDATION

Regarding the current legal provisions and their implications, particularly regarding the protection of personal data and the relatively wide scope of some provisions of the Directive 95/46/EC, an instrument must be created at the European level to make available categories of data which are actually restricted by commercial or data protection rules. This framework will facilitate, namely, the position of European agencies dealing with maritime security, allowing building data protection rules for the envisaged exchange with third states.