PROPOSED LEGAL MANUAL FOR DEMONSTRATION

"Great is the reign of the Sea"

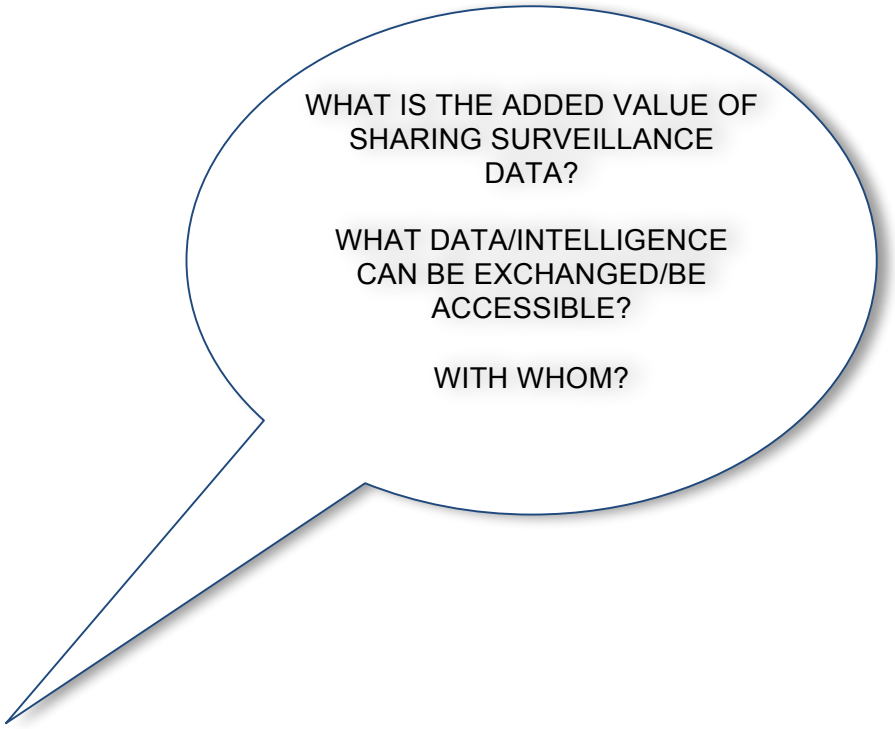
Thucydides,

Histories, Book A, verse 143.

D I S C L A I M E R

All data displayed in the demo is only for exclusive and demonstrational use. Any similarity or reference to physical or moral persons, locations, situations, or other objects or subjects of legal importance, is fictitious and clearly accidental, and if not, shall be used for educational purposes only. The use of this data by the recipients of this manual is in no way addressed in violating the interests of any entity, not party to this project.

INDEX



1. INTRODUCTION

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].

On the 10th of October 2007 the European Commission adopted a Communication[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 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 systems. In other words, this project goes beyond border related aspects, thus covering all maritime activities, such

[1] Parallel to the respective legislation of international instruments (IMO) .
[2] Convention SOLAS, Chapter XI – 2, ISPS Code.
[3] Directive 2002/59/CE.
[4] COM (2007) 575, 10/10/2007.

as maritime safety, protection of the marine environment, fisheries control and law enforcement.

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 access, 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 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 problems and solutions encountered by the parties and the ways how to resolve them.

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

[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 "need and 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.

[6] TFUE, articles 326 – 334.

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.

The main task of the legal working group, as reflected in this manual, relates to the identification and possible address of all legal problems on the exchange of certain data and/or in having such data being made available to all parties to this project. The solutions reached by the parties are to be found endorsed in the final report. Civil and military data fusion must be shared during the BMM experimentation.[7]

The main goal of this project remains that of supporting the demo phase, from the national "node" point of view, in order to each and every party to be capable of adapting to its own national perspective.

This mutual support is based on the idea of clarifying the type of access that each entity must have whilst at the same time re-establishing eventual restrictions that must be then considered on a technical and security level. At the end, this support is to serve in bridging further the process of providing access rights between the parties to this project.

ASSUMPTIONS:

- Only data types identified by the UWG on the matrix are considered for this manual and exchanged in the demo: basic and additional. The TWG shall insure that the ownership of the data is updated at any time during the development of the demonstration.
- All MS are reminded of their Data Protection obligations in the use of data.
- The ´need to know´ and ´responsibility to share´ principles are to form the basis of the demonstration.
- The demonstration aims at expressing the added value of cross sector and cross border exchange covering the field of military, law enforcement and civilian data.

[7] For example, SPATIONAV systems (military data), used in France to establish a single real maritime picture, could be enriched with additional civil data from customs authorities.

2. LEGAL DEFINITIONS[8]

"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;[9]

"processing of personal data"('processing'): 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;[10]

"controller": 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;[11]

"**recipient**": shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or

[8]IAW 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 and Decision of 27 November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
[9] Article 2 Directive 95/46/EC
[10]Article 2 Directive 95/46/EC
[11] Article 2 Directive 95/46/EC

not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients[12].

3. MANUAL DEFINITIONS

Basic data – shall mean the data Distribution Plan (UWG Matrix) as data exchanged among BMM MS.

Additional data – shall mean the UWG Matrix as data exchanged between BMM MS on a case by case basis as outlined in para 4 below.

The information to be exchanged is categorized from the access restrictions as follows:

Green: Data available for sharing in the whole BMM community.

Blue: Data available for sharing in limited sectorial communities.

Orange: Data available for sharing with respect to legal restrictions.

[12] Article 2 Directive 95/46/EC

4. LEGAL MANUAL

BASIC DATA

Positional Data

Track number or label
Position latitude and longitude
Time GMT
Course
Speed
Navigational status
Type of sensor
data provider

Current Voyage Data

Port of origin
Last port of Call
Time of Departure (ETD + ATD)
Port of destination
Estimated Time of arrival (ETA +ATA)
RoutePlan
Cargo(IMO class+ quantity)

Cargo (other than IMO class)
Draught
Total number of persons on board
ISPS level
Platform limitations

Basic ID Data

Name
Yearofconstruction
Type
Hull main color
Numberofmasts
propulsiontype
Shipmaximumspeed
Length
Beam
Max draught
Grosstonage
Deadweight
Port of registry
Flag
Ship owner*

Ship company*
IMO number
MMSI number
International RadioCall Sign
Classification society
Ship photograph*
GMDSS class
Activity

* REMINDER - Information regarding ship owner and ship company, as well as ship photograph, is to be considered as “personal data” if it relates to the identification of a “natural person”.

Other Data

Satellite Imagery*
Environmental information (detail what info) (SERV)
METOC data (SERV)
Insurrance coy
Ship agent
Environmental INCIDENT (BASIC DATA)
Safety INCIDENT REPORT (UNCLAS)(BASIC DATA)

* **REMINDER** - Information regarding satellite imagery is to be considered as “personal data” if it relates to the identification of a “natural person”.

ADDITIONAL DATA

Current Voyage Data

Events related with last port
Master/Captain details
Crew list
List of persons o/b
Elements of suspicion of the persons on board
Latest report

Historical Data

Ship name history
Ship ports history
Ship flag history
Ship ownership history
Ship routes history
Ship MMSI history
Port State control history

Elements of suspicion of the vessel

Other Data

Intelligence
ALERTS*
Infrastructure*
Elaborated Sectorial Information

*__REMINDER__: classified according to the classification of the original information/data and the classification agreed upon by the users actors.

5. 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.

The main legal instrument to be used during the demonstration are the Council Framework Decision 2006/960/JAI of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the member states of the European Union and the Convention on Mutual Assistance and Cooperation between customs administrations (Naples II).

5.1. Personal Data Protection

The main texts at the european level are :

- Directive 95/46 of the European Parliament and the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personnal data and the free movement of such data
- Council Framework Decision 208/977/JHA of 27 November 2008 on the protection of personnal data processed in the framework of police and judicial cooperation in criminal matters
- Laws relating to data protection at the national level should also be taking into account.

WARNING – Information regarding the ship agent, as well as ship photograph, is to be considered as "personal data" if it relates to the identification of a "natural person".

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.

5.2. Confidentiality and Commercial/Professional Secrecy:

WARNING - Sometimes there is contractual confidentiality that doesn't permit the information sharing (v.g. Lloyds Data Base).

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.

Confidence classification for BMM is:

1 - Very high confidence, verified data;
2 - High confidence (cooperative / non cooperative correlation);
3 - Confident (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).

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.[13]

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

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

have access to the data). Additionally, it should be taken into account that, if the sourcing of 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).[14]

5.3. Participants' 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.

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.

5.4. Persons right of access

Notwithstanding that the data processed in this demonstration refers to "non real" situations, such processing can nonetheless be lawfully extended in cases of criminal proceedings (real data i.e.); this, in line with existing EU and MS legislation.

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

5.5. Data security policy

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

a. physically protect data;
b. deny unauthorised persons access to national installations in which the Member State store data (checks at entrance to the installation);
c. prevent the unauthorised reading, copying, modification or removal of data media (data media control);
d. prevent the unauthorised inspection, modification or deletion of stored personal data (storage control);
e. prevent the unauthorised processing of data (control of data processing);
f. ensure that persons authorised to access the data have access only to the data covered by their access authorisation, 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 authorised 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 unauthorised reading and copying of personal data during their transmission, in particular by means of appropriate common protocols and encryption standards (transport control).