BLUEMASSMED LEGAL QUESTIONNAIRE - PORTUGAL

DATA/INTELLIGENCE SHARED INSIDE YOUR COUNTRY

What surveillance´s systems does your country have? (Fill this column) What entity controls each one? (Fill after the system) Do entities share data? (Fill the right columns - colours and explanations as in the stated example) (SEE SECOND QUESTIONNAIRE)	All law enforcement authorities [1]	Some law enforcement authorities (which ones?)	Other civilian entities	Other military entities
e.g. VTS (entity) (see catalogue of systems created by UG)				
AIS				
LRIT				
CleanSeaNet				
MSSIS				
SafeSeaNet				
SIVE				
VMS				
V-RMTC				
Radar				
Satellite				
(…)				
II. Do entities share this data/intelligence? (Fill the right columns - colours and explanations)				
1. Personal criminal data [2]	1	1	2	2
2. Personal criminal intelligence [3]				
a) General data	1	1	2	3
b) Information regarding incidents and violations, including those placed on black/grey lists	1	1	2	3
c) Ships involved in maritime events (including events involving their cargo or crew/owners) (e.g. any incidents, violations, detainments and inspections)	1	1	4	3
3. Data that depends on the authorization of the competent judicial authority (in camera proceeding)	5		5	5
4. Personal data (not criminal)				
a) General data	6	6	6	6
b) Information about shipping companies (e.g. commercial operator; registered owner; crew list)	7		7	7
5. Another kind of data related to surveillance information (not included in the previous nrs).				
a) General data about maritime vessels routinely detected (e.g. ship identity; current voyage data)				
b) Reference information about vessels (imagery of the ship)				
c) Reference information about vessels (cargo	4		4	4

[1] COUNCIL FRAMEWORK DECISION 2006/960/JHA of 18 December 2006 (article 2 (a)): «a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authority.»

[2] Personal data that might be related to the data subject during or prior to criminal proceedings in connection with a criminal offence or criminal proceedings and the data relating to criminal convictions. Consider the sharing of data that doesn't depend on the authorization of the competent judicial authority (in camera proceeding).
www.statewatch.org/news/2006/sep/eu-dp-council-issues-5193-06.pdf

[3] COUNCIL FRAMEWORK DECISION 2006/960/JHA of 18 December 2006 (article 2 (c)): information «which a competent law enforcement authority is entitled by national law to collect, process and analyse (…) about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future». This happens inside a «procedural stage, not yet having reached the stage of a criminal investigation».

	information including risk classification)				
d)	Information about national maritime assets that contribute to maritime surveillance (e.g. deployment schedules; routine patrol areas)	8		8	8
e)	Information about national maritime areas of focus (e.g. exclusion zones; sea routes)	9		9	9
f)	Information about land-based national maritime surveillance sensors (e.g. positional information)	9		9	9
g)	Information from national maritime ports (e.g. cargo information; running list of vessels scheduled in port and at anchor; historical data)	10		10	10

	- Data/intelligence shared
	- Data/intelligence **not** shared (legal restriction)
	- Data/intelligence **not** shared (other restriction: e.g. not linked)
	- Data/intelligence shared on a case-by-case basis (legal restriction)
	- Data/intelligence shared on a case-by-case basis (other restriction)

Explanation of all restrictions (do not forget questions / matters to be considered in the next questionnaire):
1 – IAW: art. 3 nr 2 and art. 10 of **Act 73/2009, 12th AUG**, law enforcement authorities exchange personal criminal data or intelligence, depending on their competence; art. 10 nr 1 of **Act 49/2008, 27th AUG** (criminal investigation law), law enforcement authorities cooperate among them, depending on their competence; art. 8 nr 2 of **Act 67/98, 26th OCT** – Directive 95/46/CE - (authorization from Data Protection National Commission – DPNC – is required)
2 – The ones that are not law enforcement authorities receive criminal data and intelligence on a case-by-case basis (need to know principle), if there are reasonable reasons to believe that it will contribute to detection, prevention or investigation on specific crimes. Art. 16 of **Act 53/2008, 29th AUG** (Internal Security Act) permits and recommends the cooperation with other public services
3 – The same as nr 2. Moreover, once the Navy and the Air Force have privileged access to the maritime environment, if while accomplishing their missions they gather useful personal criminal intelligence, it is handed over to the competent law enforcement authorities (see art. 2 nr 3 a) of **Act 233/2009, 15th SEP –** Navy Organization Law)
4 - The same as nr 2, although sometimes there is contractual confidentiality that doesn't permit to share information (v.g. Lloyds data base)
5 – IAW: art. 9 nrs 1 and 4 of **Act 73/2009, 12th AUG** (must be required) art. 86 of **Penal Process Code**
6 – IAW the conditions of **Act 67/98, 26th OCT – Directive 95/46/CE** - on the protection of personal data, in particular the authorization of DPNC
7 – There are two possible problems: a. Sometimes there are contractual confidentiality that doesn't permit to share information b. If the information contains personal data we have to follow note nr 6
8 – Classified information
9 – Only the information available in open sources (v.g. nautical documents) is shared
10 - Sometimes the information is not all available in web open sources; it is possible to have contractual confidentiality that doesn't permit to share information (v.g. Lloyds data base)

BluemassMed
BLUE MARITIME SURVEILLANCE SYSTEM MED
HIC ET UBIQUE

DATA/INTELLIGENCE SHARED BETWEEN BMM COUNTRIES

I. What surveillance´s systems does your country have? (Fill this column) Do your country share data? (Fill the right columns - colours and explanation as in the stated example)	All law enforcement authorities	Some law enforcement authorities (which ones?)	Homologous [4] authorities or entities	Other civilian entities	Other military entities	EU agencies	Outside EU members (v.g. Interpol)
e.g. VTS (entity) (see catalogue of systems created by UG)	A			A	A	A	A
AIS	B			B	B	B	B
LRIT	C			C	C	C	C
CleanSeaNet (EMSA)		D			D	D	
MSSIS							
SafeSeaNet (EMSA)		E			E	E	
SIVE (Guardia Civile SP)							
VMS		F		F	F	F	
V-RMTC	G			G	G	G	G
SIVICC – Sistema Integrado de Vigilância, Comando e Controlo (Guarda Nacional Republicana)		H			H		H
Radar							
satellite							
(…)							
II. Do entities share this data/intelligence? (Fill the right columns - colours and explanations)							
1. Personal criminal data	1	1		2	2	2	3
2. Personal criminal intelligence							
a) General data	1	1		2	2	2	3
b) Information regarding incidents and violations, including those placed on black/grey lists	1	1		2	2	2	3
c) Ships involved in maritime events (including events involving their cargo or crew/owners) (e.g. any incidents, violations, detainments and inspections)	1	1		2	2	2	3
3. Data that depends on the authorization of the competent judicial authority (in camera proceeding)	4			4	4	4	4
4. Personal data (not criminal)							
a) General data	5			5	5	5	6
b) Information about shipping companies (e.g. commercial operator; registered owner; crew list)	7			7	7	7	7
5. Another kind of data related to surveillance information (not included in the previous nrs).							
a) General data about maritime vessels routinely detected (e.g. ship identity; current voyage data)							
b) Reference information about vessels (imagery of the ship)							
c) Reference information about vessels (cargo information including risk classification)	8			8	8	8	8
d) Information about national maritime assets that contribute to maritime surveillance (e.g. deployment schedules; routine patrol areas)	9			9	9	9	9
e) Information about national maritime areas of focus (e.g. exclusion zones; sea routes)	10			10	10	10	10
f) Information about land-based national maritime surveillance sensors (e.g. positional information)	10			10	10	10	10

[4] "Homologous means the equivalent authority of the other country that is the primary responsible entity for the data.

g) Information from national maritime ports (e.g. cargo information; running list of vessels scheduled in port and at anchor; historical data)	11			11	11	11	11

	- Data/intelligence shared
	- Data/intelligence **not** shared (legal restriction)
	- Data/intelligence **not** shared (other restriction: e.g. not linked, political, strategic)
	- Data/intelligence shared on a case-by-case basis (legal restriction)
	- Data/intelligence shared on a case-by-case basis (other restriction)

Explanation of all restrictions (if it is a legal restriction, specify the EU or national legislation).
Add lines above with another kind of data (if is necessary to a more accurate explanation).
In your explanations, try to consider the following questions / matters:

- How is the legal framework of disclosing **confidential data** to BMM parties?
- What main restrictions exist on the sharing of data pursuant to **data protection law**? Think about the time you can keep the data without the permission of a competent entity (administrative and judicial purpose)
- What main restrictions exist on the sharing of data obtained from a third country, or to be released to a third country?
- What kind of **data security policies** does your country have? And how does it prohibit or restrict the sharing (or further use) of certain data?
- Are there any grounds of concerning **public access to documents** on which such access may be refused?
- Do any of your military entities have law enforcement authority at sea? Explain.
- Commercial or business secrecy/sensitive, secret of state, trade secret, tax secrecy, contractual confidentiality, "need-to-know" basis ... (see Legal aspects of maritime monitoring & surveillance data - final report from European Commission)

A – Exchange of information on a selective and secure basis

B - 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
VTM Directive

C – Contracting states receive information, but they can't exchange with another states. The exception is SAR information, that can be shared

D – 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 alerts the coastal state and the pollution control entity. The color will change to green, as soon as CleanSeaNet joins BlueMassMED

E - The color will change to green, as soon as SafeSeaNet joins BlueMassMED

F – This is confidential information that is exchanged between the competent authorities of:

- the flag Member State (receive VMS data through its fisheries monitoring centre (FMC))
- the coastal Member State (receive data from the flag State FMC in respect of a foreign fishing vessel in its waters)
- The European Commission (obtain remote on-line access on specific request)

Practice about sharing of VMS data at national level beyond the FMC, varies among Member States

G – The exchange of information depends on the authorization from the participantes

H – IAW **Act 63/2007, 06th NOV.** Personal criminal data or intelligence is shared in a case-by-case basis

1 – IAW **Council Framework Decision 2006/960/JHA, of 18 December 2006 (PRT Act 74/2009, of 12 August)**:
Preamble (3) – "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"
Preamble (5) -"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"
Preamble (9) – "As regards the exchange of information, this Framework Decision is without prejudice to essential national security interests, the jeopardizing of the success of a current investigation or the safety of individuals, or specific intelligence activities in the field of State security"
Article 1 nr 1. - this Framework Decision applies to existing information and intelligence inside criminal

investigations or criminal intelligence operations Article 1 nr 5. – "This Framework Decision does not impose any obligation to obtain any information or intelligence by means of coercive measures" Article 3 nr 2. – "Information and intelligence shall be provided at the request of a competent law enforcement authority" Article 3 nr 3. – "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. – "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) Article 12 nr 4. – "Member States may conclude or bring into force bilateral or multilateral agreements or arrangements after this Framework Decision has come into force in so far as such agreements or arrangements allow the objectives of this Framework Decision to be extended and help to simplify or facilitate further the procedures for exchanging information and intelligence falling within the scope of this Framework Decision" In conclusion law enforcement authorities must share criminal data and intelligence at the request of a competent law enforcement authority. Moreover, countries can conclude or bring into force bilateral or multilateral agreements or arrangements (v.g. consequence of BLUE MASSMED) that allow the objectives of this Framework Decision and that simplify or facilitate further the procedures for exchanging information and intelligence
2 - The ones that are not law enforcement authorities receive criminal data and intelligence on a case-by-case basis (need to know principle), if there are reasonable reasons to believe that it will contribute to detection, prevention or investigation on specific crimes
3 – Article 6 nr 2. (**Council Framework Decision 2006/960/JHA, of 18 December**) – "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. – "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 speciality, 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" Article 13 (**Council Framework Decision 2008/977/JHA, of 27 November**) – conditions and safeguards required to transmit data to bodies outside the EU
4 - It is necessary to submit the request to a judicial authority for an authorisation: Article 3 nr 4. (**Council Framework Decision 2006/960/JHA, of 18 December 2006**) – "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 authorisation of a judicial authority, the requested competent law enforcement authority shall be obliged to ask the competent judicial authority for an agreement or authorisation to access and exchange the information sought"
5 – IAW the conditions of **Act 67/98, 26th OCT – Directive 95/46/CE** - on the protection of personal data, in particular the authorization of DPNC
6 - IAW art. 19, nr 1 of **Act 67/98, of 26 October and art. 25 of Directive 95/46/CE**, the exchange of information outside EU "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"
7 - There are two possible problems: a. Sometimes there are contractual confidentiality that doesn't permit to share information (v.g. Lloyds data base) b. If the information contains personal data we have to follow note nr 5
8 - Sometimes there are contractual confidentiality that doesn't permit to share information (v.g. Lloyds data base)
9 - Classified information

10 - Only the information available in open sources (v.g. nautical documents) is shared
11 - Sometimes the information is not all available in web open sources; it is possible to have contractual confidentiality that doesn't permit to share information (v.g. Lloyds data base)

RECOMMENDED SOLUTIONS

Recommend possible **legal solutions for all restrictions stated above** (e.g. change national law, change EU law – in what terms?) If there is no legal solution for some information exchange, consider the **use of alerts**. What are the legal implications of an alert stating that a ship is suspected?
EU Law allows that law enforcement authorities share criminal data and intelligence at the request of another competent law enforcement authority The solution to share criminal data and intelligence without request is to conclude multilateral agreements between BLUE MASSMED countries The ones that are not law enforcement authorities receive criminal data and intelligence on a case-by-case basis (need to know principle) if there are reasonable reasons to believe that it will contribute to detection, prevention or investigation on specific crimes It is important to use an alert system in order to avoid the interference, during an investigation, of other entities that are engaged in maritime activities. For example, the Navy and the Air Force have privileged access to the maritime environment and can gather useful personal criminal intelligence, that it is handed over to the competent law enforcement authorities The alert system allows us to identify a contact as a suspect. This signal should contain the information about the entity that has the suspicion, in order to receive information

LIST OF EU LEGISLATION/DOCUMENTS RELATED TO DATA EXCHANGE

- Add relevant EU legislation or another kind of documents. If a Directive, add the correspondent internal transposition Law.
- List any bilateral or multilateral maritime information sharing agreements (formal or informal) your country has with other nations or organizations.

EU LEGISLATION

1. Lisbon Treaty
2. Council Framework Decision 2006/960/JHA, of 18 December 2006 - on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
3. 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 Data Protection
4. Regulation 45/2001/EC
5. Directive 2002/59/EC of the European Parliament and of the Council, of 27 June 2002 - establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC ("VTM Directive")
6. Directive 2003/4/EC of the European Parliament and of the Council, of 28 January 2003 - on public access to environmental information
7. Directive 2003/98/EC of the European Parliament and of the Council, of 17 November 2003 - on the re-use of public sector information
8. Transparency Regulation (EC) 1049/2011, which regulates public access to documents held by Community institutions.
9. Directive 2007/2/EC of the European Parliament and of the Council, of 14 March 2007 - establishing an Infrastructure for Spatial Information in the European Community
10. Council Framework Decision 2008/977/JHA, of 27 November 2008 - on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
11. Council Decision 2009/934/JHA, of 30 November 2009 - adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information

Isabel Dourado 10/7/12 16:24
Mis en forme: Justifié, Interligne : 1,5 ligne, Numéros + Niveau : 1 + Style de numérotation : 1, 2, 3, ... + Commencer à : 1 + Alignement : Gauche + Alignement : 0 cm + Retrait : 0,63 cm, Adjust space between Latin and Asian text, Adjust

Isabel Dourado 10/7/12 16:24
Mis en forme: Anglais (E.U.)

Isabel Dourado 10/7/12 16:24
Supprimé: .

12. Council Common Position 2005/69/JHA, of 24 January 2005 - on exchanging certain data with Interpol
13. DIRECTIVE 96/9/EC of the European Parliament and of the Council of 11 March 1996 - legal protection of databases

ANOTHER RELEVANTE LEGISLATION

14. United Nations Convention on the Law of the Sea (Montego Bay Convention 1982)
15. International Convention for the Safety of Life at Sea (SOLAS)

ANOTHER RELEVANT DOCUMENTS

16. Naples II Convention - Council Act f 18 December 1997, drawn up on the basis of Article K.3 of The Treaty on EU, on mutual assistance and cooperation between customs administrations
17. Legal aspects of maritime monitoring & surveillance data (final report from European Commission)

BILATERAL OR MULTILATERAL MARITIME INFORMATION SHARING AGREEMENTS

18. Technical Agreement on cooperation between Portugal and France regarding maritime security
19. Technical Agreement on cooperation between Portugal and Spain regarding maritime security
20. Operational Arrangement concerning the establishment of a virtual regional maritime traffic centre "5+5" network (V-RMTC 5+5 NET)

Isabel Dourado 10/7/12 16:25
Mis en forme: Sans numérotation ni puces

Isabel Dourado 10/7/12 16:25
Supprimé: .

LIST OF ACRONYMS AND ABBREVIATIONS

- AIS – Automatic Identification System
- AMASS - Autonomous maritime surveillance system
- CleanSeaNet – satellite based monitoring system for maritime oil spill detection and surveillance in European waters
- COCAE - Cooperation across Europe for Cd(Zn)Te based security instruments
- COSMO-SkyMed - COnstellation of small Satellites for Mediterranean basin Observation (Italian Space System for Earth Observation)
- DIISM-SIIMS - Dispositivo Interministeriale Integrato Sorveglianza Marittima/ System for Interagency Integrated Maritime Surveillance (Italian system)
- EMSA – European Maritime Safety Agency
- EUROSUR – European Border Surveillance System
- STIRES – SafeSeaNet Traffic Information Relay and Exchange System
- GLOBE - European Global Border Environment
- MSSIS – Maritime Safety and Security System
- LRIT – Long-Range Identification and Tracking of Ships
- SafeSeaNet – system of the European Commission
- Sat-AIS Study - Satellite AIS System Study for Maritime Safety and Security
- SECTRONIC - Security system for maritime infrastructures, ports and coastal zones
- SIVE – Sistema Integrado de Vigilância Exterior (Spanish system)
- TALOS - Transportable autonomous patrol for land border surveillance
- VMS – Vessel Monitoring System
- V-RMTC – Virtual Maritime Traffic Centre
- VTS - Vessel Traffic System