

BLUEMASSMED LEGAL QUESTIONNAIRE - ITALY

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)	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)			1	
AIS (Coast Guard)				
LRIT (Coast Guard)	4			
CleanSeaNet (Coast Guard)	4			
SafeSeaNet (Coast Guard)	4			
VMS (Coast Guard)				
V-RMTC (Navy)		5		
VTS (Coast Guard)				
C4I (Command, Control, Communication, Computers and Intelligence) (Guardia di Finanza)	6	6	6	6
A.C.S.R. (Advanced Coastal Surveillance Radar) (Guardia di Finanza)	6	6	6	6
II. Do entities share this data/intelligence? (Fill the right columns - colours and explanations)				
1. Personal criminal data ²		1 *	7	7
2. Personal criminal intelligence ³				
a) General data		1 *	7	7
b) Information regarding incidents and violations, including those placed on black/grey lists		1 *	7	7
c) Ships involved in maritime events (including events involving their cargo or crew/owners) (e.g. any incidents, violations, detainments and inspections)		1 *	7	7
3. Data that depends on the authorization of the competent judicial authority (in camera proceeding)			2	7
4. Personal data (not criminal)				
a) General data		1 *	7	7
b) Information about shipping companies (e.g. commercial operator; registered owner; crew list)		1 *	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)		1 *	7	7
b) Reference information about vessels (imagery of the ship)		1 *	7	7
c) Reference information about vessels (cargo information including risk classification)		1		






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».

d) Information about national maritime assets that contribute to maritime surveillance (e.g. deployment schedules; routine patrol areas)		2		
e) Information about national maritime areas of focus (e.g. exclusion zones; sea routes)	*	7	7	7
f) Information about land-based national maritime surveillance sensors (e.g. positional information)		2		
g) Information from national maritime ports (e.g. cargo information; running list of vessels scheduled in port and at anchor; historical data)		3		

	- 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 - Depending on due authorization of the Judicial Authority, or on need-to-know for criminal prosecution or police activity
2 - Depending on need-to-know for criminal prosecution or police activity
3- According to the data required and to the owner of the information
4- According to legal restrictions by the EU/national rules in force
5 - System not linked with other agencies or administrations
6 -Surveillance's systems used by Guardia di Finanza do not allow to share information with other national or international Administrations, having regard to their technical structure. Sharing data can be done by other means allowed by the law, such as direct requests or similar.
7 - Restrictions exclusively referred to Guardia di Finanza
* Restrictions exclusively referred to Coast Guard. According to legal restrictions of GdF these data are not shared for legal restriction (to read as a red box)

DATA/INTELLIGENCE SHARED BETWEEN BMM COUNTRIES

8 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)				1	2		
AIS (Coast Guard)						1	
LRIT (Coast Guard)						2	
CleanSeaNet (Coast Guard)						3	
SafeSeaNet (Coast Guard)						4	
VMS (Coast Guard)						5	
V-RMTC							
C4I (Command, Control, Communication, Computers and Intelligence) (Guardia di Finanza)							
A.C.S.R. (Advanced Coastal Surveillance Radar) (Guardia di Finanza)							
II. Do entities share this data/intelligence? (Fill the right columns – colours and explanations)							
1. Personal criminal data							
2. Personal criminal intelligence							
a) General data						6	6
b) Information regarding incidents and violations, including those placed on black/grey lists						6	6
c) Ships involved in maritime events (including events involving their cargo or crew/owners) (e.g. any incidents, violations, detainments and inspections)						6	6
3. Data that depends on the authorization of the competent judicial authority (in camera proceeding)						6	6
4. Personal data (not criminal)							
a) General data						6	6
b) Information about shipping companies (e.g. commercial operator; registered owner; crew list)						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)						6	6
b) Reference information about vessels (imagery of the ship)						7	
c) Reference information about vessels (cargo information including risk classification)						6	6
d) Information about national maritime assets that contribute to maritime surveillance (e.g. deployment schedules; routine patrol areas)						6	6
e) Information about national maritime areas of focus (e.g. exclusion zones; sea routes)						6	6
f) Information about land-based national maritime surveillance sensors (e.g. positional information)						6	6
g) Information from national maritime ports (e.g. cargo information; running list of vessels scheduled in port and at anchor; historical data)						6	6

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

	- 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)

1 - Shared with EMSA through the Mediterranean AIS Server

2 - Shared with EMSA as cooperative data centre

3 - Shared with EMSA

4 - Shared with EMSA

5 - Shared with CFCA

6 - Restrictions referred to Coast Guard activity. According to legal restrictions of Guardia di Finanza, these data are shared on a case-by-case basis for legal restriction (to read as a grey box)

7 - Restrictions exclusively referred to Coast Guard activity

All other restrictions in red according to EU/national rules in force, which do not allow the sharing or further use of data with third countries (the same for public access to documents). Secret of State as well as need-to-know basis add to such restrictions

The Italian Coast Guard is a branch of the Italian Navy, thus is a military administration functionally dependant on the Ministry of Defence and (for main institutional services) on the Ministry of infrastructure and transport and other Ministries (e.g. Environment; Fisheries, etc.). The Coast Guard is a maritime law enforcement administration, being entrusted with functions of maritime police - according to the Code of Navigation - for all criminal offences forecast by italian maritime laws

RECOMMENDED SOLUTIONS

Recommend the 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?

Recommended solutions by Coast Guard Headquarters

Possible legal solutions for all restrictions stated above:

- a) change national law (long and unpredictable process, due to the sovereignty of Parliament);**
- b) change EU law (long process, possible only on agreed terms between a majority of EU countries) with legal contents allowing single EU countries to share data with EU agencies or with other EU countries on a need-to-know basis: the system would require, however, some changes in national pertinent rules before implementation;**
- c) signature of ad hoc agreements, or MoUs, between EU member States and concerned EU agencies collecting relevant data, so as to allow the sharing of information for particular purposes (such agreement or MoU should involve each issue pertaining to the information exchange, so as to follow EU rules and guidelines, and would be a much faster process than the change of national or EU laws currently in force).**

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
4. 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
5. Directive 2003/4/EC of the European Parliament and of the Council, of 28 January 2003 - on public access to environmental information
6. Directive 2003/98/EC of the European Parliament and of the Council, of 17 November 2003 - on the re-use of public sector information
7. 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
8. 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
9. 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
10. Council Common Position 2005/69/JHA, of 24 January 2005 - on exchanging certain data with Interpol

ANOTHER RELEVANTE LEGISLATION

11. United Nations Convention on the Law of the Sea (Montego Bay Convention 1982)

ANOTHER RELEVANT DOCUMENTS

12. 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
13. Legal aspects of maritime monitoring & surveillance data (final report from European Commission)

BILATERAL OR MULTILATERAL MARITIME INFORMATION SHARING AGREEMENTS

14. **Italy - France bilateral operational agreement among Administrations responsible for financial and customs maritime surveillance in the Mediterranean Sea, done at Rome on 26th of February 1994**

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 - COstellation 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)
- 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 Vigilancia 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