

BLUEMASSMED LEGAL QUESTIONNAIRE

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 Customs “Gendarmerie maritime”	Other civilian entities Maritimes affairs	Other civilian entities
SPATIONAV (Navy)		4		Tous 1
V-RMTC (Navy)	2			
MSSIS (Navy)				
Satellite (DRM)				3
LRIT (DAM)				
CleanSeaNet (DAM)				
SafeSeaNet (DAM – connection to TRAFIC 2000)				
TRAFIC 2000 (DAM – connection to SPATIONAV)				
VMS (DAM)				
...				
II Do entities share this data/intelligence ?				
1. Personnal criminal data ²				

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

2. Personnal criminal intelligence ³				
a) General data				
b) Information regarding incidents and violations, including those placed on black grey lists				
c) Ships involved in maritime events (including events involving their cargo or crew /owners) (eg any incidents, violations, detentions and inspections)				
3. Data that depends on the authorisation of the competent judicial authority (in camera proceeding)		7		
4. Personnal data (not criminal)				
a) General data				
b) Information about shipping companies (eg, commercial operator, registered owner, crew list)				
5. Another kind of data related to surveillance information (not included in the previous nrs)				
a) General data about maritime vessels routinely detected (eg ; shipn identity, current voyage data)		5	5	
b) Reference information about vessels (imagery of the ship)				
c) Reference information about vessels (cargo information including risk classification)		5	5	
d) Information about national maritime assets that contribute to maritime surveillance (eg, deployment schedules, routine patrol,)		6	6	6
e) Information about land based national maritime surveillance sensors (eg, positional information)				
f) Information about land-based national maritime surveillance sensors (eg, positional information)				

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».

⁴ 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 .

g) Information from national maritime ports (eg, cargo information, running list of vessels scheduled in port and at anchor, historical data)				
---	--	--	--	--

■	- 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:
1 – Individual access to Spationav by Intradef channel is possible (need to know principle)
2 – Navy is the only french contributor to have access to international data bases ; some informations of these data bases can be share with others french services on a case by case basis .(Frenc Navy is not the cpmpetent authority in charge of these systems.)
3- Sattellites information are under control of the DRM on rrequest.
4 – « Gendarmerie maritime » is military police place for employment with the navy
5 – via SPATIONAV
6 – Maritime Prefect performs the synthesis means participating in nmaritime surveillance.
7 – recipients of data bases are judicial police officers with spécial access autorisation






Data/intelligence shared between BMM countries

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	Some law enforcement authorities)	Autorités ou entités homologues ⁴	Other civilian entities	Other military entities	EU agencies	Outside EU members (v.g Interpol))
SPATIONAV (Marine nationale)							
V-RMTC (Marine nationale)							
MSSIS (Marine nationale)							
Satellite (Marine nationale)							
LRIT (DAM)							
CleanSeaNet (DAM)							
SafeSeaNet (DAM)							
TRAFIC 2000 (DAM)							
VMS (DAM)							
...							
II Do entities share this data/intelligence ?							2
1. Personal criminal data						1	
2. Personal criminal intelligence							
a) General data						1	

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

b) Information regarding incidents and violations, including those placed on black grey lists						1	
c) Ships involved in maritime events (including events involving their cargo or crew /owners) (eg any incidents, violations, detainments and inspections)						1	
3. Data that depends on the autorisation of the competent judicial authority (in camera proceeding)						1	
4. Personnal data (not criminal)							
a) General data						1	
b) Information about shipping companies (eg, commercialoperator, registred owner, crew list)						1	
5. Another kind of data related to surveillance information (not included in the previous nrs)							
a) General data about maritime vessels routinely detected (eg ; shipn identity, curent voyage data						1	
b) Reference information about vessels (imagery of the ship)						1	
c) Réference information about vessels (cargo informationincluding risk classification)						1	
d) Information about national						1	

maritime assets that contribute to maritime surveillance (eg, deployment schedules, routine patrol areas,)							
e) Information about national maritime areas ofn focus (eg , exclusion zone, sea routes)						1	
f) Information about land-based national maritime surveillance sensors (eg, positionnal information))							
g) Information from national maritime ports (eg, cargo information, running list of vessels scheduled in port and at anchor, historical data)						1	

	- 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 (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**?
- 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?
- Secret of state, trade secret, tax secrecy, “need-to-know” basis ...

1 –At this stage, sharing informations and personnal datas with european agencies depends of every agencies statuts (As example, Frontex can not be recipient of personnal data). Others agencies are reserved on the the need to know and must take position (Ex Europol, eurojust)

2 –Legal restrictions are applicable on the Exchange data with third states of the european Union particulary in data protection rules (the adequacy of the level of protection ; consent of the member state from witch the data were obtained).

Recommend the possible **legal solutions for all restrictions stated above** (e.g. change national law, change EU law – in what terms?)?

An instrument must be created at the european level to make available catégories of data witch are actually restricted by commercial or data protection rules. This framework will facilitated the position of the european agencies concerne by maritime security and to, bulit a data protection rules for the exchange with third sates of the european union..

LIST OF EU LEGISLATION RELATED TO DATA EXCHANGE

- **Add relevant EU legislation.**
 - List any bilateral or multilateral maritime information sharing agreements (formal or informal) your country has with other nations or organizations.
1. 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
 2. 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
 3. 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
 4. Directive 2003/4/EC of the European Parliament and of the Council, of 28 January 2003 - on public access to environmental information
 5. Directive 2003/98/EC of the European Parliament and of the Council, of 17 November 2003 - on the re-use of public sector information
 6. 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
 7. 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
 8. 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
- Council Common Position 2005/69/JHA, of 24 January 2005 - on exchanging certain data

LIST OF ACRONYMS USE

- CleanSeaNet – satellite based monitoring system for maritime oil spill detection and surveillance in European waters.
- MSSIS –Maritime Safety and Security Systems
- LRIT Long range Identification and tracking of ships
- SafeSeaNet – Système of the european commission
- VMS –Vessels monitoring system
- V-RMTC –Virtuial Maritime Traffic center
- SPATIONAV
- Trafic 2000