EUROPEAN
COMMISSION

Brussels, 9.4.2021
C(2021) 2361 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 9.4.2021

on the situational pictures of the European Border Surveillance System (EUROSUR)

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 9.4.2021

on the situational pictures of the European Border Surveillance System (EUROSUR)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624[1], and in particular Article 24(3) thereof,

Whereas:

(1) Regulation (EU) 2019/1896 defines situational pictures as an aggregation of geo-referenced near-real-time data and information received from different authorities, sensors, platforms and other sources which is transmitted across secured communication and information channels and can be processed and selectively displayed and shared with other relevant authorities in order to achieve situational awareness and support the reaction capability at, along or in the proximity of the external borders and the pre-frontier area. This definition, represents a development of the concept as initially laid down in Regulation (EU) No 1052/2013[2], reflecting a more a "data centric" approach permitting users to select the appropriate graphical display and user interface depending on the operational situation and their command and control needs.

(2) Regulation (EU) 2019/1896 provides for the establishment of national situational pictures, a European situational picture and specific situational pictures to be produced through the collection, evaluation, collation, analysis, interpretation, generation, visualisation and dissemination of information. Situational pictures are to consist of three separate information layers, namely, an events layer, an operational layer and an analysis layer.

(3) It is necessary to lay down the details of each of the information layers of the situational pictures and the rules for the establishment of specific situational pictures. It is further necessary to specify the type of information to be provided and the processes governing the provision of such information as well as mechanisms to ensure quality control. In order to ensure a coordinated approach that enhances information exchange, reporting in the European Border Surveillance System ('EUROSUR') should be specified and standardised.

(4) In order to ensure that the events layer of situational pictures are sufficiently comprehensive and detailed, national coordination centres and, where applicable, the European Border and Coast Guard Agency ('the Agency') and the international coordination centres, should provide timely reports on events likely to have an impact on the external border.

---

1 OJ L 295, 14.11.2019, p. 1-131.

2 Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur) (OJ L 295, 6.11.2013, p. 11).

(5) The reporting of events through indicators and as single event reports is complementary. The indicators help assessing the overall evolution at a border section and contribute to improved situational awareness while the single event reports are linked to a timely response to a given event.

(6) Single events reports may require urgent action to be taken. It must therefore be possible to report single events in a timely manner in order to allow a timely response to such events. An initial report should be sent as soon as the event is detected and should be displayed in the corresponding situational pictures. In order to prevent delay that could undermine the capability for a quick reaction, the validation process should permit the sending of a report with a partial validation.

(7) At the same time, the issuing of reports in such circumstances can lead to false alarms. The originator and the owner of the situational picture should assess and indicate the level of confidence in the reports and in the events displayed in the situational picture. The first report should be completed with other follow up reports, as soon as supplementary information is available.

(8) The reporting of events related to document fraud and criminality in EUROSUR will complement the reporting obligations provided for in Regulation (EU) 2020/493 of the European Parliament and of the Council[3] as part of the False and Authentic Document Online system (FADO).

(9) The reporting of single events involving the cross border movement of goods and associated illicit trafficking under this Regulation should not affect existing reporting obligations, restrictions or competences concerning the customs area as well as systematic control reporting in particular under the Import Control System 2 ('ICS2') pursuant to Article 186 of Commission Implementing Regulation (EU) No 2015/2447 or risk information sharing under the Customs Risk Management System ('CRMS') pursuant to Article 86 of the same Regulation and the Customs Information System ('CIS') established by Council Regulation (EC) No 515/97. It should also not duplicate established reporting mechanisms carried out by Member States in connection with customs and customs performance matters. Where available, the relevant information could be obtained from existing Commission sources.

(10) As regards the operational layer of situational pictures, in order to ensure sufficiently comprehensive overview, the owner of situational pictures should receive reporting on Member States' own assets, reports on operational plans, as well as reports on environmental information including, in particular, meteorological and oceanographic information. In the case where the impact level at a border sections are high or critical, the need for coordination calls for a detailed reporting of the operational plans to better anticipate the response of the different authorities involved.

(11) The operational reporting to be carried out in the framework of a joint border operation or a rapid border intervention should be described in the operational plans of each joint border operation or of a rapid border intervention.

(12) As regards the analysis layer of the situational pictures, the owner of situational pictures should establish the analysis layer based on risks analysis reports. These reports aim at enhancing the understanding of events at the external border which can facilitate the forecasting of trends, the planning and conduct of border control

[3] Regulation (EU) 2020/493 of the European Parliament and of the Council of 30 March 2020 on the False and Authentic Documents Online (FADO) system and repealing Council Joint Action 98/700/JHA.

operations as well as strategic risk analysis. The methodologies related to the risk analysis reporting, and the attribution of confidence levels should be based upon the common integrated risk analysis model (CIRAM).

(13) In order to ensure consistency and facilitate information exchange while preserving security, the Agency should integrate and develop its various risk analysis networks and tools in the framework of EUROSUR, such as the Frontex Risk Analysis Network (FRAN), the European Document Fraud Risk Analysis Network (EDF-RAN) or the Maritime Intelligence Community Risk Analysis Network (MIC-RAN).

(14) Reporting in EUROSUR should take into account the specificity of certain border control activities such as air or maritime surveillance border surveillance but also the specificity of certain related events such as secondary movements or Search and Rescue incidents. The reporting of such information contributes to the establishment of the European situational picture, including risk analysis and the attribution of impact levels. In addition, reporting on search and rescue operations of migrants, both at land and at sea, should contribute to ensure the protection and saving lives of migrants.

(15) The owner of the situational picture should manage the situational picture with a view to providing a clear understanding of the situation at each external border section and for each area of responsibility, and to facilitate risk analysis and reaction capabilities at proper level.

(16) When establishing specific situational pictures with third parties to EUROSUR, Member States and the Agency should comply with and promote the technical and operational standards for information exchange developed by the Agency.

(17) It is necessary to lay down the operational responsibilities for reporting and for maintaining the situational pictures in relation with the technical responsibilities for operating and maintaining the various technical systems and networks that support the processing of information in EUROSUR.

(18) In order to ensure that operational responsibilities for the technical implementation of EUROSUR are defined in sufficient detail, it is necessary to identify the technical components of EUROSUR. In order to manage the significant amount of information processed and to reduce the workload of operators, information exchange in EUROSUR should be automated. Member States and the Agency should develop technical interfaces to foster machine to machine interconnections and use decision support tools to assist EUROSUR operators in their tasks.

(19) When defining format of reports related to the vessels of interest as part of the technical standards for information exchange, the Agency, in close cooperation with the relevant national authorities, should make use of internationally agreed formats deriving from the relevant international legislation with in the first place the UN Convention on the Law of the Sea, the Customary law of the Sea and the instruments derived notably by the International Maritime Organization (IMO) as well as their variations in the domestic legal order of the flag States.

(20) When defining format of reports related to the aircrafts of interest as part of the technical standards for information exchange, the Agency, in close cooperation with the relevant national authorities, should seek to use internationally agreed formats such as those defined by the International Civil Aviation Organization (ICAO).

(21) The data security in EUROSUR aims at ensuring the authenticity, availability, the integrity, the confidentiality and the non-repudiation of the reports and of any other data and information processed in EUROSUR.

(22) The data security of the technical components of EUROSUR corresponds to the ability of the technical components to detect and resist, at a given level of confidence, any action that compromises the security of the processed data and information, or the related services offered by, or accessible via, those networks and information systems.

(23) The data security of EUROSUR is a collective responsibility of the Member States and of the Agency.

(24) The cybersecurity threats are constantly evolving and are now more and more affordable to criminal and terrorist networks. EUROSUR should ensure an adequate and homogeneous protection against cyber threats at both EU and national levels. EUROSUR is a framework for the exchange of information covering different levels of classification. While implementing the technical components of EUROSUR, the relevant national authorities and the Agency should ensure that any user has proper access to the relevant information corresponding to his level of accreditation and his need to know.

(25) When deploying the Communication Network up to 'Confidential EU', the Agency should provide an interim solution for those national components that would be still accredited only up to 'RESTREINT UE/EU RESTRICTED' level or equivalent national classification levels.

(26) As part of the data security rules of EUROSUR and in order to ensure a proper accreditation process, this Regulation establishes a joint Security Accreditation Board ('the Accreditation Board'), within the Agency. In line with the provisions of the Commission Decision (EU, Euratom) 2015/444, such a Board is needed in the case of EUROSUR because EUROSUR is composed of several interconnected systems involving several parties.

(27) The Accreditation Board is an independent technical body which does not affect the functions of the Agency's management board.

(28) In application of the principle of subsidiarity, security accreditation decisions should, following the process defined in the security accreditation strategy, be based on local security accreditation decisions taken by the respective national security accreditation authorities of the Member States.

(29) In order for it to carry out all of its activities quickly and effectively, the Accreditation Board should be able to set up appropriate subordinate bodies acting on its instructions. It should accordingly set up a Board to assist it in preparing its decisions.

(30) Security accreditation activities should be coordinated with the work of the authorities responsible for managing the systems and other relevant entities responsible for implementing the security provisions.

(31) Given the specific nature and the complexity of EUROSUR, it is essential for the security accreditation activities to be carried out in a context of collective responsibility for the security of the Union and of the Member States, by making efforts to reach a consensus and by involving all parties with an interest in security, and for permanent risk monitoring. It is also imperative that technical security accreditation activities be entrusted to professionals who are duly qualified in the field of accrediting complex systems and who have an adequate level of security clearance.

(32) In order to ensure that the Accreditation Board is able to accomplish its tasks, it should also be provided that Member States supply the Board with any necessary documentation, grant access to classified information in the framework of EUROSUR and supporting systems (including the Communication Network) and to any areas falling within their jurisdiction to duly authorised persons, and that they should be responsible at local level for the accreditation of the security of areas that are located within their territory.

(33) While direct access to a national system is a sole prerogative of the Member State concerned, Agency staff could be granted direct access to national systems in the framework of EUROSUR to assist national authorities in their tasks.

(34) The provisions related to data security of the external components of EUROSUR should be part of the provisions related to EUROSUR in the corresponding working arrangements and model status agreements. In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2019/817 and is not bound by it or subject to its application. However, given that Regulation (EU) 2019/817 builds upon the Schengen acquis, Denmark notified on 31 October 2019, in accordance with Article 4 of that Protocol, its decision to implement Regulation (EU) 2019/817 in its national law.

(35) This Regulation constitutes a development of the provisions of the Schengen acquis in which Ireland does not take part, in accordance with Council Decision 2002/192/EC; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(36) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC.

(37) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2008/146/EC.

(38) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen acquis within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU.

(39) The measures provided for in this Regulation are in accordance with the opinion of the European Border and Coast Guard Committee,

HAS ADOPTED THIS REGULATION:

Article 1
Subject matter

This Regulation lays down:

(a) the rules for reporting in EUROSUR, including the type of information to be provided and the time limits for reporting;

(b) the details of the information layers of the situational pictures;

(c) the modalities for the establishment of specific situational pictures;

(d) the responsibilities related to the reporting, to the management of the situational pictures and for operating and maintaining the various technical systems and networks that support EUROSUR;

(e) the data security and data protection rules of EUROSUR;

(f) mechanisms for ensuring quality control.

Article 2
Scope

This Regulation applies to the information exchange and cooperation for the purposes of EUROSUR including situational awareness, risk analysis and for supporting the planning and conduct of border control operations.

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

1. 'event' means a situation, which is likely to have an impact on the external borders either as regards migration, cross border crime, or the protection and saving of the lives of migrants, including border incidents, or that may affect the functioning of EUROSUR, including any of its technical components;

2. 'managing a situational picture' means establishing and maintaining the situational picture and processing all the information that it contains;

3. 'owner' means the entity, agency or body managing the situational picture and the corresponding reports;

4. 'processing' means any action performed on the data and metadata and information contained in a report, whether those actions are automated or not, including collecting, recording, organising, structuring, storing, modifying, consulting, using, transmitting, publishing, combining, erasing, downgrading and destroying this data and metadata;

5. 'indicator' means a measurement or value that refers to events or to tasks describing the situation at external borders which contributes to situational awareness and risk analysis or supports reaction capabilities;

6. ‘technical indicator’, means a measurement or value that refers to events or to tasks which contributes to situational awareness and risk analysis related to the functioning of EUROSUR or supports corresponding reaction capabilities;

7. ‘Maritime Rescue Coordination Centre’ means a unit responsible for promoting efficient organisation of search and rescue services and for coordinating the conduct of search and rescue operations within a search and rescue region as referred to in the International Convention on Maritime Search and Rescue;

8. ‘external flight’ means any flight of a manned or unmanned aircraft and its passengers and/or cargo to or from the territories of the Member States, which is not an internal flight as defined in point 3 of Article 2 of Regulation (EU) 2016/399 of the European Parliament and of the Council [4];

9. ‘International Coordination Centre’ means the coordination structure established for the coordination of a joint operation or a rapid border intervention at the external borders;

10. ‘watchlist’ means a list of suspicious entities, assets, behaviours or profiles established on the basis of risk analysis, with a view to orient the detection and risk analysis capabilities of the European Border and Coast Guard and trigger appropriate reaction capabilities;

11. ‘the technical components’ means the systems and networks used for the purpose of EUROSUR, including the infrastructure, organisation, personnel and information resources needed to support it;

12. ‘facilitation’ means facilitation of unauthorised entry, transit and residence as defined in Council Directive 2002/90/EC;

13. ‘refusal of entry’ means a refusal of entry issued to a third-country national at external borders, in accordance with Article 14 of Regulation (EU) 2016/399, for not fulfilling all the entry conditions laid down in Article 6(1) while not belonging to the categories of persons referred to in Article 6(5) of that Regulation, and to whom a standard refusal form has been issued in accordance with Annex V of the Schengen Borders Code;

14. ‘trafficking in human beings’ means an offence referred to in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011;

15. ‘security accreditation’ means the formal authorisation and approval granted to a system or network of EUROSUR by the relevant Security Accreditation Authority (SAA) to process EUROSUR data in its operational environment, following the formal validation of a Security Plan and its correct implementation;

16. ‘operational status’ means the ability of an asset, unit, system or centre to perform its operational function(s) characterised as ‘fully operational’, ‘limited operational functions’, or ‘not available’;

17. ‘a sublayer’ means a layer of information underneath the event layer, the operational layer or the risk analysis layer of a situational picture.

---

[4] Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (OJ L 343, 29.12.2015, p. 558).

CHAPTER I
Principles of reporting in EUROSUR

SECTION 1
GENERAL PRINCIPLES

Article 4
Reports in EUROSUR

1. Reports shall be transmitted between two or more entities, units, bodies or agencies for the purposes of contributing to the establishment of the different situational pictures, to contribute to risk analysis, or to support reaction capabilities.

2. Reports shall be composed of:

   (a) data containing the basic information;

   (b) meta-data containing additional information that contributes to the understanding of the dataset in a wider context and supports its processing in EUROSUR.

3. Reports may take the form of:

   (a) indicators as referred to in Article 8;

   (b) single event reports as referred to in Article 9;

   (c) reports on own assets as referred to in Article 10;

   (d) reports on operational plans as referred to in Article 11;

   (e) reports on environmental information as referred to in Article 12;

   (f) risk analysis reports as referred to in Article 13;

   (g) requests for information as referred to in Article 14;

   (h) watchlists as referred to in Article 15.

Article 5
Roles in reporting

1. The national coordination centres, the European Border and Coast Guard Agency ('the Agency') or the entities managing the specific situational pictures, referred to as "the originators of the reports", shall transmit reports in EUROSUR.

2. The owner of the situational pictures, referred to as the "owners", shall be the recipients of the report and shall be responsible for processing it in accordance with the applicable rules.

3. Reports in EUROSUR may originate from the national sources referred to in Article 25(2) and Article 26(2) of Regulation (EU) 2019/1896 or from the Agency's own sources.

Article 6

Links

1. Where the originator of a report establishes a relationship between reports or with other elements of the situational picture that can facilitate the understanding of the overall situation and context, it shall link this report to the relevant elements.

2. The owners of a situational picture may add or modify the links related to the situational picture he is managing.

SECTION 2
EVENT REPORTING

Article 7

Reporting events in EUROSUR

1. Each national coordination centre shall ensure that the national authorities of Member States responsible for border management, including coast guards to the extent that they carry out border control tasks, report in the event layer of relevant situational pictures all events detected while conducting border control activities, performing situational awareness and risk analysis as well as events related to unauthorised secondary movements, where available.

2. When carrying out border control tasks, the Agency and, where relevant, the international coordination centres shall be subject to the obligation referred to in paragraph 1.

3. Events in EUROSUR shall be reported as indicators or as single event reports or both.

Article 8

Indicators on events at external borders

1. The national coordination centres and, when relevant and as provided for in the operational plans, the international coordination centres, shall report indicators on events at external borders to the Agency as set out in Annex I and provided at the times specified in that annex.

2. The data corresponding to the indicators may be derived from information and statistics available to national authorities including through searches of relevant Union databases and large-scale information systems, in accordance with the legal framework applicable to those databases and systems.

3. Indicators relating to illicit cross border movement of goods and associated illicit trafficking shall be obtained in cooperation with competent national authorities taking due account of other reporting obligations or restrictions and the role of the Commission.

4. In addition to the reporting obligation referred to under paragraph 1, an originator of a report may send a specific report:

   (a) to alert on an abnormal change of the values observed;

   (b) to inform on a specific modus operandi or pattern which has been detected;

(c) in the case of situations referred to in point (b), the report may be linked to a specific risk analysis.

5. Where the Agency obtains any of the indicators referred to in paragraph 1 by its own surveillance assets or through cooperation of the Agency with Union institutions, bodies, offices and agencies and international organisation or cooperation of the Agency with third countries, it shall report the indicators in the European Situational Picture and shall inform the national coordination centres thereof. In this case and for these indicators, the reporting obligation of Article 7 (1) shall not apply.

Article 9

Single events reports

1. The national coordination centres and, when relevant and as provided for in the operational plans, the international coordination centres, shall report the single events to the Agency.

2. Single events shall be reported in EUROSUR wherever:

(a) a timely reaction is needed for to the single event;

(b) the specific event has an impact on external borders which is high or very high; or

(c) the event is listed in Annex 2.

3. Unless specified otherwise in Annex 2, the originator of the report shall send the first report on the event no later than 24 hours after relevant competent authority became aware of an event has occurred or is likely to occur.

4. The originator of the report shall submit additional reports as appropriate for the purpose of complementing or updating a single event report. They shall be linked to the initial single event report and to the event reported in the situational picture.

5. Reports prepared under this Article shall contain a description of the response of the authorities to the events reported, including any action taken or planned to be taken.

6. Without prejudice to the first operational response, the owner of the report and the originator of the report may request further information and risk analysis as provided for in Article 14, in order to:

(a) complete the information corresponding to the event;

(b) increase the confidence level referred to in Article 16;

(c) update the impact level attributed;

(d) update the situation related to the event.

7. On the basis of the reports received, the owner of the situational picture may close the event where it is considered that:

(a) the suspected event did not take place;

(b) the estimated impact of the event does not justify the reporting;

(c) the situation described in the event has ended.

In case an event is closed, the event and the various reports linked to it shall be stored and shall remain accessible in the situational picture for risk analysis purposes.

8. Where the Agency obtains sufficient information on single events by its own surveillance assets or through cooperation of the Agency with Union institutions, bodies, offices and agencies and international organisation or cooperation of the Agency with third countries, it shall report this information in the European Situational Picture and shall inform the national coordination centres thereof. In this case, the reporting obligation of paragraph 1 shall not apply.

9. The Agency shall include or update these events as appropriate in the European situational picture.

SECTION 3
OPERATIONAL REPORTING

Article 10
Reports on own assets

1. Each national coordination centre and where applicable the relevant international coordination centre and the Agency shall ensure that their units participating in border control operations report on own assets in the European situational picture.

2. The reports on own assets in EUROSUR shall comprise:

   (a) the operational status of the national coordination centres including their ability to perform the tasks listed in Article 21(3) of Regulation (EU) 2019/1896 and, when relevant, the operational status of the international coordination centres. Any significant change in operational status of the national coordination centre shall be reported to the Agency in real time;

   (b) the position and operational status of the command and control centres used for border control operations;

   (c) the areas of responsibility for border surveillance and for the checks at border crossing points;

   (d) the type and distribution of border control units and their status.

Article 11
Reports on operational plans

1. Each national coordination centre shall ensure that the units participating in border control operations report their operational plans in the national situational pictures.

2. National coordination centres, and, where relevant, the international coordination centres, shall report the operational plans in the European situational picture where the impact levels at the borders sections are high or critical or in the case of joint border operations/ rapid border interventions.

3. The reports on operational plans shall contain:

   (a) a description of the situation;

   (b) the operational aim and the anticipated duration of the operation;

   (c) the geographical area where the operation is to take place;

   (d) a description of the tasks, responsibilities and special instructions for the teams and units participating, with modus operandi and objectives of the deployment;

(e) the composition of the deployed staff including numbers of staff deployed and their profiles;

(f) command and control plans, including the operational status of the command and control centres, the function performed and corresponding systems and communication tools;

(g) the technical equipment to be deployed, including specific requirements such as conditions for use, requested crew, transport and other logistics;

(h) the schedule of border surveillance patrols, including the patrolling area and number of assets engaged;

(i) detailed procedures on event reporting.

Article 12

Reports on environmental information

1. The relevant authorities, services, agencies and programmes at national and EU level may report environmental information in the operational layer of the relevant situational pictures.

2. The reporting on environmental information in EUROSUR may contain:

(a) real-time images provided by video cameras, radar systems and other detection devices;

(b) meteorological observations and weather forecasts;

(c) oceanographic information and drifting model services;

(d) geospatial products;

(e) other operational pictures, which may help understand the situation at external borders or monitor a specific border operation.

SECTION 4
RISK ANALYSIS REPORTING

Article 13

Reports related to risk analysis

1. The national coordination centres, the Agency and, where relevant, the international coordination centres, shall ensure the provision of risk analysis reports with a view to updating the analysis layers of the situational pictures.

2. The risk analysis reports shall include one or more of the following: analytical products such as briefing notes, analytical reports, third country analysis and risk profiles, and specific earth observation reports using geospatial information systems.

3. The risk analysis reports shall be used for:

(a) facilitating the understanding of events and incidents at external borders and, where available, their relation to unauthorised secondary movements and the analysis and forecast of related trends;

(b) facilitating the targeted planning and conduct of border control operations;

(c) strategic risk analysis.

Article 14

Request for information

1. Where there is a need to obtain further reports on a specific event, or to update the situational picture, the national coordination centres, the Agency or the entities managing the specific situational pictures, may send a request for information to one or several sources referred to in Article 25(2) and 26(2) of Regulation (EU) 2019/1896.

2. A request for information made pursuant to paragraph 1, may be subject to a classification level or other specific data policy restrictions.

3. The risk analysis reports in response to a request for information shall be linked to the original request for information.

4. The principle of originator's consent shall apply both to the requests for information and to the reports made in response thereto.

Article 15

Watchlists

1. The Agency shall establish and maintain watchlists for the purposes of enhancing the detection and risk analysis capabilities of the European Border and Coast Guard and trigger appropriate reaction capabilities.

2. Watchlists shall be composed of:

   (a) entities, assets, behaviours or profiles, which, on the basis of risk analysis, are suspected to be connected with illegal immigration and cross-border crime, or that may endanger the safety of life of migrants;

   (b) a suggested reaction in case of detection, including data policy restrictions applicable to the reports.

3. Watchlists may include:

   (a) suspected vessels;

   (b) suspected aircrafts;

   (c) suspected airports of origin, and other places known or suspected to be places of origin of external flights;

   (d) suspected ports of origin, anchorages, awaiting berths and other places known or suspected to be places of origin of maritime traffic;

   (e) suspected operators.

SECTION 5

PROVISIONS COMMON TO THE "EVENTS LAYER" AND THE "RISK ANALYSIS LAYER"

Article 16

Confidence levels

1. The originator of an event report or of a risk analysis report shall assess the confidence level in the reported information as part of the metadata forming part of the report.

2. The confidence level shall be assessed on the basis of the following criteria:

(a) the credibility of the reported information;

(b) the reliability of the source;

(c) the validation status of the report.

3. The owner shall take into account the confidence level associated with the report to update the situational picture accordingly.

Article 17

Attribution of impact levels

1. The originator of an event report or of a risk analysis report shall assess the impact level of the reported information as part of the metadata forming part of the report.

2. The impact level shall reflect the overall impact of the reported information on:

(a) the detection, prevention and combating of illegal immigration;

(b) the detection, prevention and combating of cross border crime;

(c) the protection of and saving the lives of migrants.

3. Originators of a report referred to in paragraph 1 shall attribute an impact level to each event and risk analysis report.

4. Where a report relates to an event already reported in the situational picture, the originator shall link the report to that event.

5. Owners shall attribute an impact level to the events or modify them based on the reports received and on their own risk analysis.

SECTION 6
REPORTING IN THE CONTEXT OF SPECIFIC BORDER CONTROL ACTIVITIES

Article 18

Reporting related to unauthorised secondary movements

Where this information is available, Member States shall:

(a) display the analysis related to unauthorised secondary movement on their territory in a specific sublayer of the national situational picture. This specific sublayer shall be shared with the Agency;

(b) report single events related to unauthorised secondary movements as provided for in Article 9, in line with their national procedures;

(c) report specific indicators related to unauthorised secondary movements.

Article 19

Reporting related to maritime border surveillance

1. Each national coordination centre shall ensure that the units participating in maritime border surveillance report on vessels:

(a) suspected of carrying persons circumventing or intending to circumvent checks at border crossing points, where such circumvention relates to illegal migration;

(b) suspected of being engaged in smuggling activity by sea or other cross border crime related activities;

(c) in cases where lives of migrants could be at risk;

(d) on the watchlists or which are subject to requests for information. In the case of reports relating to point (d), the reporting shall take into account the data policy restrictions provided for in Article 14 (2) and Article 15 (2) (b).

2. The participating unit shall transmit the information to its own national coordination centre and, in the case of a joint operation or a rapid border intervention, to the corresponding international coordination centre in accordance with the operation plan.

3. The national coordination centres and, when relevant, the international coordination centres shall update their respective situational pictures and report this information to the Agency with a view to update the European situational picture.

Article 20

Events related to Search and Rescue at sea

1. While performing maritime border surveillance, Member States authorities rendering assistance to any vessel or person in distress at sea, in accordance with their obligation under international maritime law shall take into account and transmit all relevant information and observations related to a potential Search and Rescue incident to the respective responsible Maritime Rescue Coordination Centre and inform their national coordination centre with a view to updating that event in the relevant situational pictures.

2. If Member States authorities clearly establish that the Search and Rescue incident is not related to the protection and saving of migrants' lives or to cross border crime, they may decide not to inform the national coordination centre.

3. While performing maritime border surveillance operations and in accordance with Regulation (EU) No 656/2014, the Agency shall be subject to the same obligation as the one referred to in paragraph 1.

4. During a Search and Rescue operation, the competent national coordination centre shall update the national situational picture and report this information to the Agency with a view to update the European situational picture.

5. The situational pictures shall be regularly updated:

(a) to support the planning and conduct of the next operational phase once the Search and Rescue operation is concluded;

(b) to assess the impact levels attributed to the corresponding incident and to the overall maritime border section;

(c) to update the relevant indicators referred to in Article 8.

6. The competent national coordination centre shall report to the Agency about the termination of a Search and Rescue operation at the latest within 24 hours after the operation is terminated.

Article 21

Reporting related to air border surveillance

1. Each national coordination centre shall ensure that the national agencies and bodies involved in air border surveillance report on external flights:

   (a) suspected of carrying persons circumventing or intending to circumvent checks at border crossing points, if the incident relates to illegal migration;

   (b) suspected of being engaged in smuggling by air or other cross border crime;

   (c) where lives of migrants could be at risk;

   (d) on the watchlists or which are subject to requests for information. In the case of reports relating to point (d), the reporting shall take into account the data policy restrictions provided for in Article 14 (2) and Article 15 (2) (b).

2. The national agencies and bodies involved in air border surveillance shall transmit that information to their own national coordination centre or, in the case of a joint operation or a rapid border intervention, to the corresponding international coordination centre in accordance with the operational plan.

3. The national coordination centre or the international coordination centre shall update their respective situational pictures and report this information to the Agency with a view to update the European situational picture.

SECTION 7
REPORTING QUALITY CONTROL IN EUROSUR

Article 22

Reporting quality of data in EUROSUR

To monitor the quality of data in EUROSUR the Agency shall establish and maintain the following indicators:

   (a) the number and frequency of reports received per border section and per border crossing points;

   (b) the timeliness of the reporting;

   (c) the completeness and consistency of the reports.

Article 23

Reporting quality of service in EUROSUR

1. In monitoring the technical and operational functioning of EUROSUR in accordance with Article 23 of Regulation (UE) 2019/1896, The Agency, in close cooperation with the competent national authorities, may establish technical indicators and the requirements for single event reporting, to monitor the operational status and quality of service offered by the various systems and networks of Member States and of the Agency connected to and forming part of the technical component of EUROSUR as defined in Article 27.

2. The indicators shall be used:

   (a) to monitor the status of the various technical components of EUROSUR in real time;

(b) to support the identification and response to incidents and failures identified in the functioning of EUROSUR;

(c) to ensure the data security of EUROSUR.

3. The Member States and the Agency shall report on any single incident affecting the technical components of EUROSUR or the data security of EUROSUR.

CHAPTER II
Situational pictures

Article 24
Structure of the situational pictures

1. The event and analysis layers of the European situational picture shall contain a sublayer on unauthorised secondary movements. Where available, event and analysis layers of the national situational picture and of the specific situational picture shall also contain sublayers on unauthorised secondary movements, for the purpose of understanding migratory trends, volume and routes.

2. The operational layer of the European situational picture shall contain sublayers on the technical functioning of EUROSUR. These sublayers shall describe:

(a) the operational status of the national coordination centres and international coordination centres;

(b) the main technical elements contributing to the functioning of EUROSUR and their status;

(c) the quality of data and the quality of service in EUROSUR;

(d) the incidents and events affecting the technical functioning of EUROSUR;

(e) the data security incidents.

3. The situational picture shall comprise other specific sublayers of information in order to facilitate the display of information to the users.

4. Each situational picture shall be established in a document specifying the layer and sublayers and the applicable data policy.

Article 25
Management of the situational pictures

The owner of the situational picture shall:

(a) process the reports received;

(b) establish and maintain the event layer of the situational picture, generate and update the events in the event layer of the situational picture and attribute corresponding impact levels, and confidence levels;

(c) establish and maintain the operational layer of the situational picture based on the reports on owns assets and reports on operational plans;

(d) establish and maintain the analysis layer of the situational picture based on the risk analysis reports and attribute corresponding impact levels and confidence levels;

(e) establish and maintain the links between the different elements of the situational picture taking into account the links in the reports;

(f) manage user access to the situational picture and contribute to the data security of EUROSUR;

(g) transmit the relevant reports and necessary information to the owners of other situational pictures, in line with Chapter 1;

(h) archive and delete the relevant information in line with the applicable data policy.

Article 26

Rules for establishing and sharing a specific situational picture

1. When establishing a specific situational picture in accordance with Article 27 of Regulation (EU) 2019/1896, Member States and the Agency shall ensure alignment with:

   (a) the principles of reporting set out in Chapter 1;

   (b) the requirements regarding the structure and management of situational pictures set out in Articles 24 and Article 25;

   (c) the general provisions set out in Chapter 3.

2. The rules for establishing and sharing a specific situational picture shall contain:

   (a) the content and scope of the specific situational picture, including:

      i. the purpose of the specific situational picture,

      ii. the information layers and sublayers,

      iii. the type of information to be reported in the specific situational picture, including event reports, operational reports and risk analysis reports;

   (b) the governance of the specific situational picture, including:

      i. the owner,

      ii. the bodies, offices and agencies that can be originators of the reports,

      iii. the rules for reporting,

      iv. provisions related to data security, including user access;

   (c) the rules for information exchange with the other users of EUROSUR, including:

      i. the mechanisms to exchange information with national and European situational pictures and the mechanisms to ensure the originator's consent,

      ii. the rules for the provision of EUROSUR Fusion Services referred to in Article 28 of Regulation (EU)2019/1896 and the corresponding procedures,

      iii. other aspects related to the technical functioning of EUROSUR, including the interconnection of the external component supporting the establishment of the specific situational picture with the relevant national or European components of EUROSUR.

Chapter III
General provisions

SECTION 1
ENTITIES RESPONSIBLE FOR THE TECHNICAL ASPECTS

Article 27
Technical components of EUROSUR

1. The technical components of EUROSUR shall include national components and a European component.

2. Each national component shall be composed of the national systems and networks used by Member States for the establishment of the situational pictures, reporting, situational awareness, risk analysis, and for supporting the planning and conduct of border control operations, including the infrastructure, organisation, personnel and information resources needed to support it. The interconnections among and between components inside a Member State as well as between Member States shall be part of the national components.

3. The European component shall complement the national components. It shall include the interconnection with the national components. It shall comprise the Communication Network and the systems and networks used by the Agency for the establishment of the situational pictures, reporting, situational awareness, risk analysis, and for supporting the planning and conduct of border control operations.

Article 28
Technical responsibilities of the Agency

The Agency shall be responsible for managing the European component, which shall include:

(a) the definition of technical standards for interconnecting networks, systems, applications and equipment of the national and external components with those of the European component;

(b) the certification process of the networks, systems, applications and equipment with a view to connecting them to EUROSUR, in close cooperation with the responsible authorities;

(c) the service management of the systems and networks used by the Agency for the establishment of the situational pictures, reporting, situational awareness and risk analysis and for supporting the planning and conduct of border control operations;

(d) the reporting of the operation, the quality service and the service management aspects of the systems and networks referred to in point (c), as provided for in Article 23;

(e) the data security of the European component.

Article 29
Technical responsibilities of the Member States

1. Each Member State shall be responsible for:

(a) managing its national component, including service management, ensuring the coordination of the connection of national systems and networks used for the establishment of the situational pictures, reporting, situational awareness, risk analysis and for supporting the planning and conduct of border control operations;

(b) reporting the operation and the quality of service and the service management aspects of the systems and networks referred to in point (a), as provided for in Article 23;

(c) the compliance with the technical standards established by the Agency;

(d) the data security of the national component.

2. The national coordination centre shall:

(a) support the coordination, planning and implementation of the national component;

(b) contribute to the regular monitoring of the quality of service and quality of data, and report it to the Agency;

(c) ensure the operational reporting on the systems and networks of the European component.

Article 30
External components

1. An external component of EUROSUR shall be composed of the systems and networks, including the infrastructure, organisation, personnel and information resources needed to support it, that are not part of EUROSUR and which:

(a) exchange data and information with EUROSUR;

(b) support the establishment of a specific situational picture.

2. The interconnection of an external component to EUROSUR belongs to the external component. It shall be specified in the rules establishing the relevant specific situational picture.

SECTION 2
DATA SECURITY AND DATA PROTECTION RULES FOR EUROSUR

Article 31
General Principles of EUROSUR data security

1. EUROSUR data security shall encompass the management and the technical activities necessary to achieve an appropriate level of protection for handling EUROSUR data and information, cope with the evolving threat environment and enable the various national bodies and agencies involved in EUROSUR and the Agency to fulfil their mission. EUROSUR data security shall include information assurance, physical security, personal security and industrial security.

2. EUROSUR data security shall comprise:

(a) security risk management, including security controls and plans, and associated monitoring, evaluation, maintenance, improvement, reporting, awareness and training;

(b) business continuity and disaster recovery, including impact assessment, continuity and recovery controls and plans, and associated monitoring evaluation, maintenance, improvement, reporting, awareness and training;

(c) security incident response and cooperative response between the Agency and the Member States for security incidents;

(d) security accreditation;

(e) user access control;

(f) data security related aspects of the planning of border operations and of the planning of information systems;

(g) security aspects of the interconnections of components;

(h) handling of classified information for the purpose of EUROSUR.

Article 32

Governance of EUROSUR data security

1. The Agency shall ensure the overall security of EUROSUR, duly taking into account the need for oversight and integration of security requirements in each component of EUROSUR.

2. The Agency shall be responsible for the data security of the European component.

3. Each Member State shall be responsible for the data security of its national component.

4. The Agency and the Member States shall ensure alignment of the controls, the processes and the plans, so that the data security of EUROSUR is horizontally and effectively assured, based on a global security risk management process.

5. The responsibilities for the data security of the external component shall be set out in the agreements, arrangements and operational plans establishing the specific situational picture, as provided for in Article 26.

6. The Agency shall adopt standards laying down the security functional requirements and the security assurance requirements for controlling the access to, and handling of, technologies that provide security to EUROSUR.

7. Each Member State and the Agency shall ensure that the necessary steps are taken to comply with the standards referred to in paragraph 6, that adequate reasoning for fulfilment of the requirements and for controlling of the risks is documented and that any further requirements related to the security of the systems are met, taking full account of expert advice.

8. Each Member State and the Agency shall report in EUROSUR any security incident affecting the data security of EUROSUR as part of the reporting on data quality and quality of service.

9. Wherever the security of the Union or its Member States may be affected by the operation of EUROSUR:

(a) the Agency shall immediately inform the relevant national coordination centres;

(b) the executive director of the Agency may decide to take any appropriate measure to remedy the situation, in close coordination with the Member States concerned, including the disconnection of certain systems and networks from the European component of EUROSUR.

Article 33

Application of security rules in EUROSUR

1. When handling EUROSUR data and information, each Member State and the Agency shall ensure that security controls, processes and plans are in place, ensuring a degree of protection which shall at least be equivalent to that guaranteed by the Commission's rules on security set out in Commission Decision (EU, Euratom) 2015/444 and Commission Decision (EU, Euratom) 2015/443.

2. Member States shall immediately inform the Commission and the Agency of the adoption of national security rules relevant for EUROSUR as referred to in paragraph 1.

3. Natural persons resident in third countries and legal entities established in third countries may deal with EUROSUR data only where they are subject, in those countries, to security rules ensuring a degree of protection at least equivalent to that guaranteed by the equivalent rules on security of the Commission.

4. The equivalence of security rules applied in a third country may be recognised in an agreement with that country.

5. As part of the implementation of the European component of EUROSUR, the Agency shall support the corresponding exchange of EUROSUR reports and the interconnection of national components both at unclassified level and at classified level.

Article 34

Principles of security accreditation in EUROSUR

The security accreditation activities shall be carried out in accordance with the following principles:

(a) security accreditation activities and decisions are to be undertaken in a context of collective responsibility for the security of the Union and of the Member States;

(b) efforts shall be made for decisions to be reached by consensus and for all relevant parties with an interest in security issues to be involved;

(c) tasks shall be carried out in respect of relevant security rules and accreditation standards applicable to the Agency, the Member States' authorities and the Commission;

(d) a permanent monitoring process shall ensure that security risks are known, security measures are defined to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in the applicable security rules and that these measures are applied in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated;

(e) security accreditation decisions shall, following the process defined in the security accreditation strategy, be based on local security accreditation decisions taken by the respective national Security Accreditation Authorities (SAAs) of the Member States;

(f) the technical security accreditation activities shall be entrusted to professionals who are duly qualified in the field of accrediting complex systems, who have an appropriate level of security clearance, and who shall act objectively;

(g) security accreditation decisions shall be taken independently of the Agency and of the entities responsible for implementing the national components of EUROSUR. The data security accreditation authority for EUROSUR shall be, within the Agency, an autonomous body that takes its decisions independently;

(h) security accreditation activities shall be carried out while reconciling the requirement for independence with the need for adequate coordination between the Agency and the national authorities responsible for implementing security provisions in Member States.

Article 35

EUROSUR Security Accreditation Board

1. A EUROSUR Security Accreditation Board ('the Accreditation Board') is established within the Agency.

2. As security accreditation authority, the Accreditation Board shall, with regard to security accreditation for EUROSUR, be responsible for:

   (a) defining and approving a security accreditation strategy for EUROSUR including the European component;

   (b) Member States shall report to the Accreditation Board regarding the accreditation of their national components, so as to ensure that the Accreditation Board can take relevant interconnection decisions;

   (c) taking security accreditation decisions for the European component, taking into account the advice provided by national entities competent in security matters and the overall security risks;

   (d) approving relevant documentation relating to security accreditation;

   (e) advising, within its field of competence, the Agency and the Member States in the establishment of security operating procedures ('SecOps'), and providing a statement with its concluding position;

   (f) examining and approving the security risk assessment cooperating with the Agency, Member States and the Commission to define risk mitigation measures;

   (g) checking the implementation of security measures in relation to the security accreditation of the European component by undertaking or sponsoring security assessments, inspections or reviews;

   (h) endorsing the selection of approved products and measures and of approved cryptographic products used to provide security for the European component of EUROSUR and for interconnection;

   (i) approving or, where relevant, together with the relevant entity competent in security matters, participating in the joint approval of:

i. the interconnection of the European component with national components,

ii. the interconnection of the external components to EUROSUR;

(j) agreeing with the relevant Member State the procedures relating to access control;

(k) on the basis of the security risk reports, informing the Agency of its risk assessment and providing advice to the Agency on residual security risk treatment options for a given security accreditation decision;

(l) carrying out the consultations which are necessary to perform its tasks.

3. In the security accreditation strategy referred to in point (a) of paragraph 2, the Accreditation Board shall set out the following:

(a) the scope of the activities necessary to perform and maintain the accreditation of the European component of EUROSUR, and their potential interconnection with other components;

(b) a security accreditation process for the European component with a degree of detail commensurate with the required level of assurance and clearly stating the approval conditions;

(c) the role of relevant stakeholders involved in the accreditation process;

(d) an accreditation schedule compliant with the deployment of the EUROSUR standards, in particular as regards the deployment of infrastructure, service provision and evolution;

(e) the principles of the security accreditation of the national components to be performed by national entities of the Member States competent in security matters;

(f) the provisions related to data security of the external components of EUROSUR.

4. The Accreditation Board shall perform its tasks independently when handling files, performing system security audits, preparing decisions and organising its meetings.

Article 36

Functioning of the Security Accreditation Board

1. The Accreditation Board shall be composed of one representative per Member State and two representatives from the Commission.

2. The security officer of the Agency shall be a designated secretary of the Accreditation Board.

3. The Accreditation Board shall establish its rules of procedure and appoint its chairperson.

4. If there is no consensus, the Accreditation Board shall have recourse to majority voting.

5. The Accreditation Board may set up subgroups to investigate technical matters.

6. The Accreditation Board shall keep the management board of the Agency and the executive director of the Agency and the Commission informed of any of its decisions.

Article 37

Role of Member States and the Agency with regard to the Accreditation Board

Member States and the executive director of the Agency shall:

(a) transmit to the Accreditation Board all information they consider relevant for the purposes of security accreditation;

(b) permit duly authorised persons appointed by the Accreditation Board to have access to any classified information and to any areas/sites related to the security of systems falling within their jurisdiction, in accordance with their national laws and regulations, and without any discrimination on ground of nationality, including for the purposes of security audits and tests as decided by the Accreditation Board;

(c) be responsible for the accreditation of their components of EUROSUR, and report, to this end, to the Accreditation Board.

Article 38

User access

1. Without prejudice to Article 35, the entity responsible for a component of EUROSUR shall manage user access to its systems networks and application.

2. In case a national staff member would be given direct access to a system or application of the Agency used for the purpose of EUROSUR, the Agency shall coordinate access rights with the relevant National Coordination Centre.

3. In case, an Agency staff member would be given direct access to a national system or application used for the purpose of EUROSUR, the responsible Member State shall coordinate access rights with the executive director of the Agency.

Article 39

Data security of the external components of EUROSUR

1. The external components may be connected to EUROSUR only if their data security is equivalent to the data security of EUROSUR.

2. The rules for establishing and sharing a specific situational picture referred to in Article 26 shall include provisions for data security, specifying the type of information that may be exchanged and the level of classification.

3. Any interconnection of an external component to EUROSUR shall be subject to the prior approval of the Accreditation Board.

Article 40

Data protection Rules for EUROSUR

1. Although data processed by EUROSUR may exceptionally contain information relating to indirectly identifiable natural persons, such data shall not be processed in the framework of EUROSUR to identify these natural persons.

2. Where the processing of information in EUROSUR exceptionally requires the processing of personal data other than ship and aircraft identification numbers, these personal data shall be deleted as soon as the purpose for which they have been collected has been achieved.

Article 41
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels, 9.4.2021

For the Commission
The President
Ursula VON DER LEYEN