Version 14/03/2024

Summary of the Data Protection Impact Assessment

of the European Banking Authority on a central database concerning anti money laundering and terrorist financing (EuReCA)

1. Project name

Development of a Data Protection Impact Assessment (DPIA) for the establishment of a European reporting System for material CFT/AML weaknesses (EuReCA) in fulfilment of the mandate conferred on the EBA under Article 9a (1) and (3) of the EBA Regulation[1].

2. Review

Review cycle:

A review of the Data Protection Impact Assessment is foreseen within a cycle of two years, starting when the system will have started to collect personal data. In case significant changes are planned to the processing operations, such as a modification of controller or co-controllership, the inclusion of additional recipients or a modification of interconnexions with other databases, an extraordinary review of the DPIA will be performed.

3. Summary

Main findings of the DPIA

The purpose of the database foreseen in Article 9a of the EBA Regulation is to process information on financial sector operators, which in most cases are not natural persons[2]. The processing of personal data is thus limited. However, in cases where the processing involves natural persons, the impact on their fundamental rights may be high, due to the nature of data collected in the context of money laundering and terrorism financing: processing of individuals data in breach of data protection principles may have a severe impact on their reputation and on their possible exclusion from social/contractual benefits and may also result in undue judicial proceedings against them.

For these reasons, controls and mitigation measures are foreseen, as further developed in this DPIA and in particular in section (iv) 'Security', which

- limit to the strict minimum the collection of identifiable information to the exhaustive list Annex II of the RTS.
- foresee a marking of personal data, independent from other sets of information collected, triggering enhanced protection and safeguards, including their redaction where relevant and ad hoc retention periods.
- secure the channels of communication with other authorities and foresee encryption of the database at rest and in transit.

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, OJ L 331, 15.12.2010, p. 12.

[2] Information related to legal persons may also constitute personal data subject to GDPR/EUDPR, insofar as they relate to identified or identifiable natural persons. This is expected to be the exceptional case, with personal data typically being related more directly to a natural person.

- limit the sharing of personal data with other authorities and ensure that such sharing is operated manually (no automated sharing).
- ensure additional quality and reliability controls by reporting authorities for such information, including special categories of data.

The final outcome of the assessment allows for a significant limitation of the likelihood and severity of the risks to individuals. Specific attention has been put on the security risks connected to the sharing of data with a large number of reporting authorities, and to the protection of sensitive data.

Description of processing:

The EBA collects information from reporting authorities in the context of preventing and countering money laundering and terrorist financing. The information relates to weaknesses identified during ongoing supervision and authorisation procedures concerning financial sector operators, as well as measures taken by reporting authorities in response to these material weaknesses.

This information is centralised in a database controlled by the European Banking Authority in compliance with Article 9a (2) of the EBA Regulation and Commission Delegated Regulation (EU) 2024/595.

The data are analysed and shared, on a need to know and confidential basis[3], with reporting authorities at national and EU level for their supervisory activities (Article 9a (2) and (3). They are used to assess ML/TF risks on an aggregate basis (Article 9a (3) and 9a (5)), and more broadly to support the EBA's role to lead and coordinate the prevention and countering of money laundering and terrorist financing in the EU, in compliance with the requirements of Article 9a of the EBA Regulation. The data will be transmitted where appropriate to national judicial authorities and the European Public Prosecutor's Office (EPPO) as specified in section (v) 'Sharing of data' of this DPIA.

The central database operates in the wider context of close coordination between the EBA and other reporting authorities at national and EU level, including the European Central Bank (ECB) and Single Resolution Board (SRB). In that context, data including personal data can also be shared on a case-by-case basis with EIOPA and ESMA as part of the general duty of cooperation foreseen in Article 2 (4) of EBA Regulation and with national Financial Intelligence Units (FIUs) pursuant to Article 9a (1a) of EBA Regulation.

EBA determines together with the reporting authorities some of the essential elements of the data processing (the type of data that shall be reported to the EBA and the conditions of their reporting). In view of the qualification as co-controllership under the EUDPR and the GDPR, their respective obligations and responsibilities in terms of data protection which are not already clearly

[3] As set out in Article 9a of the EBA Regulation and in line with Annex II of the RTS and particular with Annex II (5) 'The dissemination of personal data by the EBA:

'When requested by a reporting authority, the EBA shall share personal data under the conditions referred to in point 4(c) of this Annex, and on its own initiative under the conditions laid down in Article 10(1), point (b), if the information about the person concerned is necessary for the reporting authority for its supervisory activity with regard to the prevention of the use of the financial system for the purpose of money laundering or terrorist financing. In both cases, the information shall be shared between authenticated users and secured communication channels shall be used.

set out in Union or Member State law are therefore specified in an arrangement[4].This covers for example responsibilities in terms of data subjects' rights including requests for access or rectification, notification of data breaches, and where relevant the assessment on a regular basis of the need to keep data in an identifiable form.

4. Reason for this DPIA

A DPIA is performed to assess the impact of the processing of the personal data of the data subjects on their fundamental rights to privacy and data protection of individuals concerned, and to determine whether the mitigation measures taken sufficiently limit the risks to the rights of individuals.

This part lists the aspects of the processing which are likely to have a significant impact on the outcome of the threshold assessment, and which explain why a DPIA is performed.

The scope of the processing is the collection of data concerning financial operators, which are both legal and natural persons. In practice, in the vast majority of cases a legal person is concerned. While private individuals are not the target of the processing, some personal data will be included in the database (see Title 7. below). The following elements affect the assessment of the impact of the central database on individuals:

- Data are collected from a large number of reporting authorities, at national and EU level. It can be considered that the central database processes data on a large scale.
- Some data may be of a sensitive or "highly personal nature" (i.e.: administrative investigations, data on politically exposed persons) according to the criteria set by the EDPS in his Decision of 16 July 2019 on DPIA lists[5].
- Some data may be shared with law enforcement authorities (national and EU), which means that special categories of data may be processed in connection with (suspicions of) criminal convictions and offences, requiring the adoption of specific safeguards.
- In order to avoid unnecessary duplication in the collection of data, as foreseen in Article 9a (1) of EBA Regulation, the EBA may in the future import data from existing databases or platforms it already controls. In particular, the EUCLID database controlled by the

[4] EDPS guidelines on the concepts of controller, processor and co-controllership under Regulation (EU) 2018/1725 of 7 November 2019 « In some cases, these roles and responsibilities are (partially) already determined by law, e.g. in the stablishing act for an information system. In fact, Article 28 of the Regulation confirms that **EU legislation can directly provide for an allocation of roles and responsibilities between the parties**. Where this is the case, there is no obligation to conclude an arrangement insofar as the respective responsibilities of the joint controllers are determined by Union or Member State law. Consequently, a clear allocation of responsibilities should be made in the operative part of the relevant legislative act (or - regarding Union law - at the latest in an implementing or delegated act, where provided for in the basic act). (…) **Unless Union law already allocates their responsibilities, the joint controllers need to enter into a specific arrangement**, **containing a clear and transparent allocation of responsibilities**. Such arrangement may take the form of a Memorandum of Understanding (hereinafter MoU) or a contract. A Service Level Agreement (hereinafter SLA) may be used in addition to the MoU as providing technical specifications. Furthermore, an SLA may be considered sufficient as an arrangement between joint controllers as long as this contains all of the elements in line with the Regulation. »

[5] Decision of the EDPS of 16 July 2019 on DPIA lists issued under Articles 39 (4) and (5) of Regulation (EU) 2018/1725, available at https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf

EBA may be used in a second phase to avoid unnecessary duplication in the collection of data[6]. This means that a matching or combination may be considered. However, this is not foreseen at the moment of the drafting of this DPIA.

A DPIA is therefore performed, taking into account the large scale of the database, the fact that sensitive and special categories of personal data may be processed and further shared, and the possible combination in the future of data from different data sets.

5. Description of processing

a. Data flow diagram of the process

(i) Source of the data

National and EU reporting authorities[7] as mentioned in Article 9a (1a) of the EBA Regulation, and further detailed in Article 1 of Commission Delegated Regulation (EU) 2024/595.

The RTS applies with regard to financial sector operators defined in Article 2 (1a) of Regulation (EU) No 1093/2010.

In practice, at national level, authorities listed in Article 1 of the RTS are as follows:

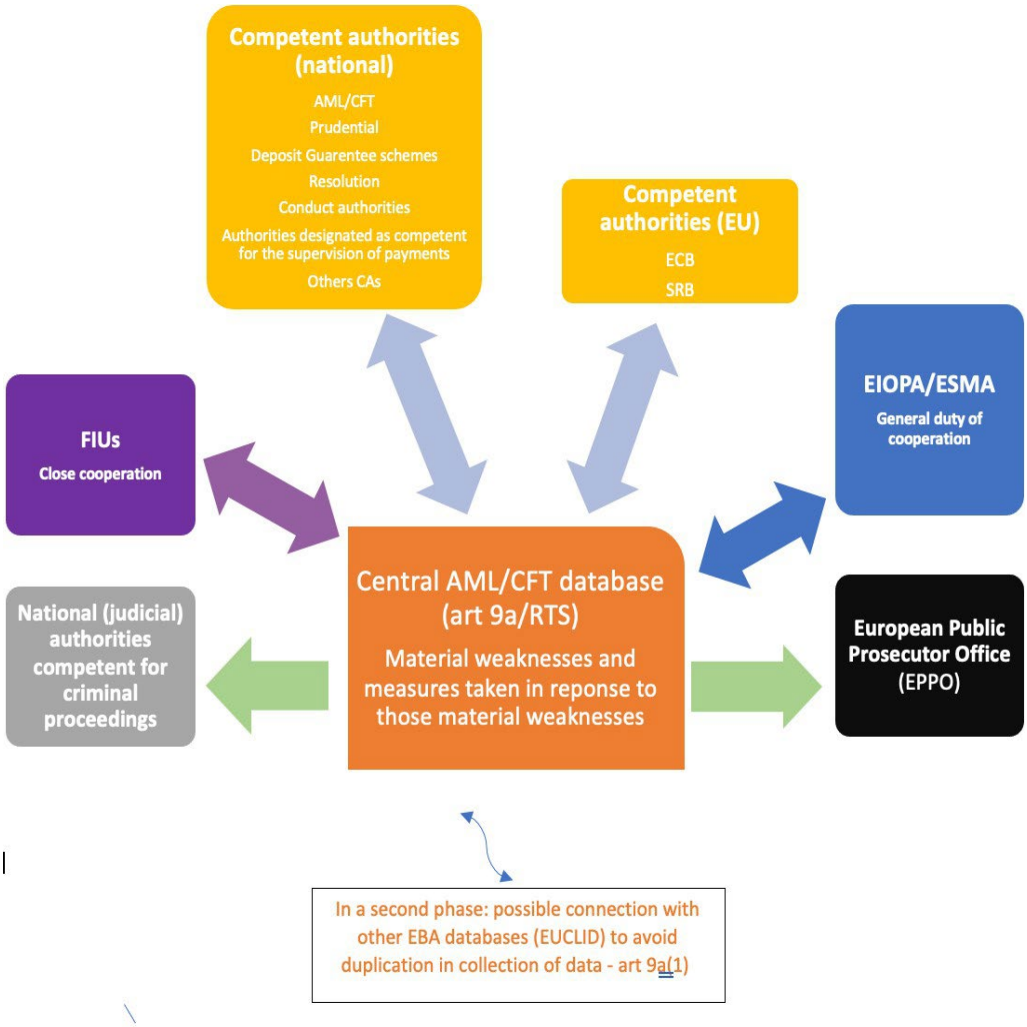
- Authorities competent for anti-money laundering and countering terrorist financing;
- Prudential authorities;
- Payment institutions authorities;
- Authorities competent for “conduct of business” compliance;
- Authorities competent for “deposit guarantee schemes” compliance;
- Resolution authorities.

Information can also be shared in the context of close cooperation with Financial Intelligence Units (FIUs).

At European level, the source of data are the European Central Bank and the Single Resolution Board. In the context of their general duty of cooperation, the information exchange also applies to the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

[6] The scope in terms of data protection is rather limited. This relates to legal persons when the name of the legal person identifies a natural person.

[7] For the detail of reporting authorities, see the annex to this document.



(ii) Categories of personal data:

As mentioned above, identification of natural persons is not the main purpose of the database. Personal data may be included in some specific fields, in case an individual has a direct connection with the materiality of the weakness identified and there is a request by EBA to identify some categories of natural persons (see below). The data necessary to make sure the right person is identified may be collected in structured fields: name, surname and date of birth, nationality, country of residence.

Personal data include information identifying a legal person (financial sector operator), when the name of the legal person identifies a natural person[8], and information relating to a natural person (customer or beneficial owner[9], member of the management body and key function holder), when such legal and natural persons have a link with a material weakness.

Categories of *personal data* will be processed as follows:

- Identification data
- Special categories of data / data of a highly personal nature: data relating to administrative sanctions and possibly connected to (suspicions of) offences, data on politically exposed person[10] in connection to the identification of material weaknesses[11], and measures taken in response to these weaknesses by reporting authorities.

Categories of *persons* are identified in annex II of the RTS as follows:

1. Member of a management body assessed as not meeting the requirements on fitness and propriety (Article 5 (2b) RTS).
   (a) Name, surname, date of birth, country of residence, nationality, function in the financial sector operator or branch;
   (b) Grounds of money laundering or terrorist financing.
2. Customer, beneficial owner, member of the management body or key function holder linked to the material weakness (Article 6 (m) RTS):

[8] ECJ, Schecke, point 53 « Legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons. » See also EDPS opinion of 13 April 2012 on a Proposal for a Council decision on the conclusion of the Agreement between the European Union and Canada with respect to matters related to supply chain security: « As the EDPS has also stated in the context of his Opinion on EU-US customs cooperation, this type of cooperation implies that some of the information exchanged will include personal data. (…) Although most of the information exchanged will relate to legal persons, personal data will be processed especially if the trade operator itself is a natural person or if the official name of the legal person acting as operator identifies a natural person. The Schecke judgment of the Court of Justice of the EU underlined the importance of data protection in such cases. Where the official name of the legal person identifies one or more natural persons the legal person can claim protection of the right to the protection of personal data ».

[9] A 'beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least the elements of Article 3(9) of Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (5AMLD).

[10] Under Article 3(9) of Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (5AMLD), a "politically exposed person' means a natural person who is or who has been entrusted with prominent public functions and includes the following:
(a) heads of State, heads of government, ministers and deputy or assistant ministers;
(b) members of parliament or of similar legislative bodies;
(c) members of the governing bodies of political parties;
(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
(e) members of courts of auditors or of the boards of central banks;
(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
(g) members of the administrative, management or supervisory bodies of state-owned enterprises;
(h) directors, deputy directors and members of the board or equivalent function of an international organisation.
No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;"

[11] see Article 3 of Commission Delegated Regulation (EU) 2024/595.for the definition of 'a material weakness'

(a) Customer or beneficial owner:

i. name, surname, date of birth, country of residence, nationality;

ii. whether the customer or beneficial owner is or was also a member, of the management body or a key function holder in the financial sector operator or branch;

iii. whether the customer or beneficial owner holds or held, directly or indirectly, shares in the financial sector operator or branch;

iv. whether the customer is considered as 'high risk' is considered as 'high risk' by the financial sector operator, branch, agent or distributor.

(b) Member(s) of the management body or key function holder(s)

i. name, surname, date of birth, country of residence, nationality;

ii. function in the financial sector operator or branch.

(c) Any natural person referred to in points 2(a) or (b) of this Annex: The reason why the reporting authority considers that the natural person appears to be linked with the material weakness.

3. Natural persons concerned by measures taken in response to a material weakness (Article 7d of the RTS):

(a) Name, surname, date of birth, country of residence, nationality;

(b) Function in the financial sector operator, branch, agent or distributor or, with regard to the customer or beneficial owner, role;

4. Information to be submitted by a reporting authority when making a request to the EBA about a natural person (Article 10 (3) (a) RTS)):

(a) Name, surname, date of birth, nationality, country of residence;

(b) Where known, the function, or, with regard to the customer or beneficial owner, role;

(c) The reason why the information about that specific person is necessary for the requesting reporting authority for its supervisory activity with regard to the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and the intended use(s) of the information requested.

5. Implementation of the data collection within Reporting authorities and EBA:

- Reporting authorities: name, surname, function, and business contacts of the person designated as responsible for the submission, the requests and the reception of information under the RTS, and name, position, and contact details of the person(s) designated as contact point(s) for such submission, requests and reception of information
- EBA: name, surname, function and business contacts of persons responsible for the reception, the processing and the sharing of information under the RTS.

(iii) Processing

The processing consists of the collection, the analysis and further sharing of the data collected, for the purpose of preventing the use of the financial system for the purpose of money laundering or of terrorist financing.

The information will be made available to reporting authorities on a need-to-know and confidential basis and transmitted where relevant to national judicial authorities and the EPPO.

Details of the processing:

- Collection of data on material weaknesses from reporting authorities. Data are pushed manually[12] by reporting authorities to the EBA via an interface set up by the EBA.
- Centralisation of the data in the EBA AML/CFT database foreseen in Article 9a (2) of EBA Regulation
- Analysis of the data collected with the purpose of examining material weaknesses and measures taken in response to these weaknesses, as described in b. below.
- Sharing of data on a case-by-case basis with reporting authorities, with FIUs in the context of close coordination with the EBA, ESMA and EIOPA in the context of institutional cooperation, and with national judicial authorities and EPPO when the information could give rise to criminal proceedings (see v. below).
- Use of the data by the EBA in carrying out its own tasks under the legal basis of Article 8 and Article 35 of Regulation (EU) No 1093/2010, and in particular its leading, coordinating and monitoring role in relation to preventing and countering ML/TF in the financial system under Article 9a of that Regulation and requesting under Article 9b of that Regulation investigations by reporting authorities of possible breaches of Union law where the data provides indications of material breaches and the EBA's broader tasks including promoting convergence of supervisory processes referred to in Directive (EU) 2015/849 (Article 9a (4) of EBA Regulation).

(iv) Storage:

As provided in Article 14 of the RTS, the EBA may keep personal data on an identifiable form for a period of up to 10 years from the collection by the EBA and, where it does so, shall delete personal data upon expiry of that period. This retention period is justified by the retention periods applied to these data by supervisory authorities when performing their supervisory functions. This varies among the Member States from 5 to more than 20 years. Concerns regarding breaches of AML/CFT requirements by EU financial institutions in recent years have involved situations that developed over periods exceeding 5 years and, in some cases exceeding 10 years.

While Article 40 of the AMLD provides as a general rule for a 5-year retention period for obliged

[12]Manual insertion of information in the database is organised in a similar way as for the central register within the field of payment services : see art 6 Commission delegated Regulation 2019/411

entities, paragraph (1) and (2) explicitly provide that an additional 5 years period may be used for further retention of personal data. AMLD does not, however, specify supervisory retention periods.

Data will be stored exclusively within the EEA, as developed in d. below. At the end of the ten years period, personal information will be deleted. Based on a regular assessment of their necessity, personal data may be deleted before the end of that maximum period on a case-by-case basis. Assessment of the accuracy and necessity of the data on a case-by case-basis will be performed on a yearly basis. As personal data are uploaded by reporting authorities in their capacity as co-controllers and as they are the ones able to verify the quality of data, a reminder will be sent every year by the EBA to reporting authorities to request that they confirm that the personal data they have uploaded, including special categories of data such as suspicions of offences and criminal convictions, are still relevant, accurate and up-to-date.

Outside this annual cycle, reporting authorities can request amendment/deletion of personal data ad hoc, e.g. when they become aware of changes to the information, or to align with domestic retention periods as the information is no longer necessary. This would be the case for instance where a reporting authority includes historical information in the database, which means that it should be retained for a period shorter than the default 10 years.

(v) Sharing of data:

The data are shared with reporting authorities:

- on a need to know and confidential basis, within the EuReCA platform, based on a reasoned request of the reporting authority and after assessment of the request by the EBA.
- on EBA's own initiative, based on its analysis: the data may be shared with relevant reporting authorities on a case-by-case basis.

Recipients of the data:

- Within the EU
  - National reporting authorities under Article 9a of EBA Regulation, as specified in the RTS, for their supervisory activities with regard to the prevention of the use of the financial system for the purpose of money laundering or terrorist financing. The information may be shared where relevant via AML/CFT and prudential Colleges.
  - FIUs, in the context of close coordination as referred to in Directive (EU) 2015/849 (Article 9a (1) a et b EBA Regulation)
  - National judicial authorities and other reporting authorities when information could give rise to criminal proceedings in accordance with national procedural rules (Article 9a (2) of EBA Regulation)[13].
- EU entities

[13] *Article 9a of the EBA Regulation: '(…) The Authority may, where appropriate, transmit evidence that is in its possession which could give rise to criminal proceedings to the national judicial authorities and the competent authorities of the Member State concerned in accordance with national procedural rules. The Authority may also, where appropriate, transmit evidence to the European Public Prosecutor's Office where such evidence concerns offences in respect of which the European Public Prosecutor's Office exercises or could exercise competence in accordance with Council Regulation (EU) 2017/1939.'*

- EU reporting authorities
  - SRB
  - ECB

  The sharing of information with SRB and ECB takes place under their general roles as reporting authorities as defined in Article 2 of the RTS and is governed by the provisions of the RTS and by the EBA Regulation.

- Others:
  - ESMA in the context of institutional cooperation
  - EIOPA in the context of institutional cooperation
  - EPPO for evidence concerning offences in respect of which the EPPO exercises or could exercise competence under Council Regulation 2017/1939.

  Data can be shared with the ESMA and the EIOPA under the conditions foreseen in Article 9 (4e) of the RTS, as part of the general duty of cooperation foreseen in Article 2 (4) of EBA Regulation.

b. Detailed description of the purpose(s) of the processing

Data are collected and further processed with the purpose of identifying and analysing material weaknesses in the supervision of activities of financial operators and vulnerabilities and risks in relation to money laundering and terrorist financing in the financial sector.

The identification and analysis of the weaknesses will enable the EBA to take several actions under Article 9a and 9b of EBA Regulation, all based on its broader mandate (Article 8 EBA Regulation) to lead and coordinate the prevention and countering of money laundering and terrorist financing in the EU:

- Analysis on an aggregate basis for the purpose of risk assessments and for adoption of an opinion on money laundering and terrorism financing risks on the basis of Article 9a (3) and (5) of the EBA Regulation.
- Promoting convergence of supervisory processes referred to in Directive (EU) 2015/849 (Article 9a (4) of EBA Regulation).
- Sharing of data on a case-by-case basis for specific supervision and enforcement actions with competent authorities, sharing of data with ESMA EIOPA and FIUs in the context of close coordination, and with national judicial authorities and EPPO when the information could give rise to criminal proceedings (see above 7a(v)).
- Requesting investigations in accordance with Article 9b of EBA Regulation.

c. Description of interactions with other processes

The process relies on personal data being fed in from other systems

Personal data will be fed in from existing systems handled by authorities competent for AML/CFT at national and EU level listed in point 7.a(i). of this DPIA. They will be uploaded on the EuReCA platform by contact persons selected in each reporting authority, using the infrastructure detailed in 7.d.

The EBA may, with a view to avoid duplication of data collection as provided in Article 9a (1) EBA Regulation[14], import some data from databases or platforms it already controls. However, such interconnexion is not foreseen in the present development of the platform. If it is envisaged in the future, the DPIA will further clarify how data may be fed in from such databases or platforms and include a comprehensive legal analysis on purpose compatibility and a technical and organisational explanation of the system interactions.

Re-use of personal data in other processes

Data stored in the EuReCA database will be made available by the EBA to reporting authorities, including ECB and SRB, on a need-to-know and confidential basis[15] and transmitted where relevant to national judicial authorities and the EPPO, outside the EuReCA platform.

As mentioned in 4. above, the process will also result in interactions and sharing of data outside of the EuReCA platform with EIOPA and ESMA under Article 9 (4e) of the draft RTS and as part of the general duty of cooperation foreseen in Article 2 (4) of EBA Regulation and with FIUs pursuant to Article 9a (1b) of EBA Regulation.

The purpose of such transmission and further use is directly connected to the purpose of the setting up of the database, i.e. administrative and judicial proceedings concerning the countering of money laundering and terrorist financing.

Data may also be used by the EBA in furtherance of its broader public interest tasks set out in Article 8 of the EBA Regulation.

d. Description of the supporting infrastructure: filing systems, ICT etc.[16]

The database is hosted within the EEA and is operated by EBA staff with restricted access rights, as developed below.

(i) Submission of data

The EuReCA Platform is used by contact points assigned by each reporting authority to submit AML/CFT data manually.

Submission of data can be done directly or indirectly:

[14] '*In developing those technical standards, the Authority shall consider the volume of the information to be provided and the need to avoid duplication. It shall also set out arrangements to ensure effectiveness and confidentiality".*

[15] Further explanations on how confidentiality is ensured on page 16 of the DPIA

[16] References:

- *Security measures:* https://edps.europa.eu/sites/default/files/publication/16-03-21_guidance_isrm_en.pdf
- *Accountability toolkit, part II, as of page 15:* https://edps.europa.eu/sites/default/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf
- *Guidelines on IT governance and IT management, with a focus on the design and testing phase as of p.18* https://edps.europa.eu/sites/default/files/publication/it_governance_management_en.pdf

- Direct submitters have access to the platform. This applies to AML/CFT authorities and prudential authorities (including ECB and SRB)
- Indirect submitters (art 12(4) RTS) have to submit data through the AML/CFT authority in charge of the supervision of the entity concerned by the material weakness. This applies to payment institution authorities, conduct of business authorities, resolution authorities and designated authorities. This communication between the indirect submitter and the reporting AML/CFT authority happens outside the EuReCA platform, and it is the responsibility of the AML/CFT authorities and indirect submitter to ensure proper channels of communication.

(ii) Functionalities

Essential functionalities of the platform include:

- Creation of an Entity (Financial Sector Operator and Establishment);
- Submission of a Material Weakness;
- Submission of a Measure;
- Commenting and updating on existing submitted items.

The functionalities on natural persons will be added in EuReCA only when the RTS have entered into force and in line with the provisions in the joint-controllership arrangements.

(iii) Users' rights

Users have read-write access, additionally to navigating and reading the content of the EuReCA platform, and can:

1. create Entities to report related Material Weaknesses and Measures
2. create Material Weakness to submit to EBA for previously created Entities
3. create Measures to submit to EBA for previously created Material Weaknesses
4. review and reply to comments from EBA in related submissions
5. upload information where needed when reporting Material Weaknesses or Measures, and submit subsequent developments.

Users submit and request information in accordance with the type of reporting authority(ies) to which they have been assigned, i.e. AML/CFT authorities, prudential Authority, including ECB and Single Resolution Board.

(iv) Security

This chapter summarises the measures and controls listed in the IT document "DPIA controls vs requirements". It should also be read in conjunction with the EBA security policy and the applicable information security framework. Limitation of the processing of personal data:

- For the collection of information, the interface is used by contact persons identified in each reporting authority, with a strictly defined structure including predetermined fields for the users to feed in the database.
- The interface is fed in manually by the users.
- Users have at their disposal a Manual that includes inter alia the functionalities

regarding the addition of natural persons information in EuReCA.

- There is a limited number of free text fields in the application.
- Warning messages appear in natural persons related free-text fields (e.g. in the Additional Information field) to inform users on the limitation of uploading of personal data to what is strictly required, and to the applicable security safeguards.
- The application will mark the fields and/ or sections with personal data appropriately so that it is clear to the users which fields will hold personal data.
- Warning message will appear when users add attachments for inclusion of personal data.
- The relevance of personal data is manually assessed on a regular basis with annual reminders to reporting authorities so that they ensure data are still up-to-date, and data are manually deleted if no longer relevant, with a maximum retention period of 10 years. Personal data have an expiry date. These verifications will apply to FSOs identifying natural persons and data listed in annex II of the RTS.
- Personal data will not be shared with authorised recipients (Reportings authorities and EU entities) in an automated way. Sharing of personal data will be assessed on a case-by-case basis and will be operated manually. This means there will be no bulk sharing of personal data via the platform, but creation of PDF, CSV or excel files for each specific case. All personal data which are not necessary will be redacted before sharing. When the sharing of personal data is necessary, it will take place via the creation of an ad hoc document including security and confidentiality safeguards as described below.
- Reasoned requests must document the relevance of the information requested.

Confidentiality:

- The system is designed to be safeguarded against deliberate and intrusive threats from internal and external actors (malicious or otherwise).
- It can only be accessed using two factor authentication, from user with specific data access permission and using passwords compliant with EBA security policy.
- Reporting authorities only have access to personal data they have uploaded.
- All extractions from the system that include personal data regarding natural persons, including PDFs created for export, support file encryption and password protection. EBA's information security policy requires information about financial sector operators, including related personal data, to have appropriate security marking and to be stored in restricted locations and circulated with encryption.
- Personal data are not exported in mixed content reports.
- Files including personal data are exported either via the platform (for reporting authorities), or outside the platform (for instance for ESMA and EIOPA) using secure communication channels.
- The system keeps an audit of all login attempts. The Security Plan provides for ensuring that activity on the system leaves a record that allows reliable after-the-fact investigations of security incidents. It foresees the forwarding of audit logs to specialised monitoring tool(s) to enable alerting and incident investigation.
- IT Operations access/ view of personal data is under exceptional circumstances for vetted individual only.
- It uses data encryption complaint with FIPS 140.3 - L3 standard.

– It logs and monitors the activity through a central SIEM for security alerts.

Integrity:

- Reporting authorities are responsible for the accuracy and quality of data they upload in the system.
- Quality control of the data submitted may be performed by the AML/CFT team who when reviewing the data submitted, and if needed, ask for clarifications. An annual reminder will also be sent to reporting authorities to ensure that data are accurate and up-to-date.
- Changes to the submitted data are only allowed by authorised and authenticated logged in users, in situations the AML/CFT team requests amendments.
- Changes to the data are visible to other authorised logged in users (within the same authority and with the same role) at the time of the changes.

Availability:

- Full back-ups are made every 24h so that the maximum amount of data loss in case of disaster is 1 working day.
- Unusual/unexpected attempts of access (internal or external) are monitored, and a break glass access protocol allows operational staff to provide emergency production operational support.
- All parts of the infrastructure are at least n+1 redundant.
- Measures have been taken so that the system can be available within 24 hours (during week days) of an unplanned outage.
- A yearly disaster recovery exercise is foreseen.
- Personal data are kept up to date with a report showing when data have been created, updated and deleted after 10 years. The retention period for personal data is applied manually independently of other data processed in the system.

Organisational measures:

- A procedure has been set up to ensure identification, analysis and evaluation of the information security risks potentially affecting personal data and the IT systems supporting their processing. Risk assessments follow ITSRM methodology which is heavily used within the EUIs.
- A disaster recovery plan will be at the disposal of the support team.
- Resources and staff have been assigned roles to perform the risk assessment.
- A security breach policy and procedure has been adopted.
- A policy for personal data breach handling has been adopted.
- The joint controllership arrangement specifies that the parties shall provide each other with reasonable assistance as required to facilitate the handling of any data breach under the EUDPR, and that each party is responsible for personal data breaches that occur as a result of an infringement of that party's obligations.
- The security measures are regularly reviewed and updated in relation to the context of the processing and the risks.

- Regular penetration tests are planned for both application and systems.
- An access control policy has been adopted where all access rights requirements are being described, including regular access reviews, and relevant roles and responsibilities.
- Vendor's best practices have been adopted during solution design of the systems.

6. Necessity and proportionality

a. The proposed processing operations are necessary for the EBA to fulfil the mandate assigned to it:

Personal data are in limited cases necessary for the analysis of weaknesses as foreseen in Article 9a of EBA Regulation and in the RTS. This is the case when:

- The identification of a material weakness in the context of AML/CFT is linked to a natural person[17].
- Measures taken by a reporting authority regarding a weakness concern a natural person. This is the case especially when a legal person identifies a natural person: personal details have to be registered even though the private person is not the primary target of the system.
- Personal data is a necessary part of the information which may give rise to criminal proceedings for which national judicial authorities or the EPPO are competent.
- At the administrative level, the proper functioning of the database requires that a contact point is identified in each authority responsible for feeding the system.

b. The processing stays inside what is proportionate for the fulfilment of that task:

Only personal data strictly required in the scenarios described above will be collected:

- At the occasion of the collection of the data, material and organisational safeguards will be put in place to prevent the uploading by users of unnecessary personal data, using technical measures described in 7.d above and in the table below, and appropriate security measures will be put in place.
- At the occasion of the analysis of data by the EBA, measures are taken to ensure accuracy and reliability.
- At the occasion of the sharing of data, safeguards consist of the fact that data are only communicated manually on a case-by-case basis, following a reasoned request or on the EBA's own initiative. Article 9a (3). stresses that only relevant data should be shared and provides for an obligation of transparency on the kind of information that is shared[18].

[17] Information related to legal persons may also constitute personal data subject to the GDPR/EUDPR, insofar as they relate to identified or identifiable natural persons. This is expected to be the exceptional case compared with personal data which more directly concerns a natural person.

[18] « The Authority shall inform the competent authority, or any other authority or institution that has initially provided the requested information, of the identity of the requesting competent authority, the identity of the financial sector »

- At the occasion of the different stages of collection and further sharing, security safeguards are in place to prevent that information is corrupted or that a security breach affects the transmission of data (see 7d. above and the table below).

It is considered that the data processed are within the limits of what is needed for the EBA to fulfil its mandate, and that the risks to fundamental rights are proportionate to the benefits of the processing activities. This is the case because, on the one hand, the purpose of the processing, which is to fight money laundering and terrorist financing, is an objective of public interest of particular importance, and on the other hand, as developed above, the personal data processed have been reduced to a minimum and safeguards taken contribute to reducing the risks concerning data subjects so that any severe impact appears unlikely.

7. Analysis of risks and establishment of controls for identified risks

Introduction to the methodology

The severity and likelihood assessments are based on the following scoring:

Level of risks on a scale of 1 to 5:
Severity: 1 = negligible, 2 = limited, 3 = moderate, 4 = Important, 5 = maximal
Likelihood: 1 = remote, 2 = unlikely, 3 = possible, 4 = likely, 5 = certain

The numbers suggested in the columns are based on the fact that:

- Personal data is not at the core of the processing, thus in general the likelihood of the risk is low (between 2 and 3) and even lower after the controls have been put in place.
- The likelihood is considered higher for processing under the responsibility of reporting authorities (compared to EBA), because of the number of reporting authorities and actors involved.
- Despite the fact that personal data are not the main focus of the data processing, if an event however affects the data, then the severity/impact may be high because of the sensitivity of the personal data processed. This explains why the severity scores higher than the likelihood in the two columns.
- The severity is considered particularly high in the context where personal data (and especially special categories of personal data) would wrongly be shared with third parties.

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls[19]	Severity (residual)	Likelihood (residual)
1	Submission of personal data by reporting authorities	Excessive or inadequate data	Purpose limitation, data quality	3	3	Technical safeguards in the interface developed for the transmission of data: Strict limitation of free text, breakdown of items for better formatting and preference for enabling the user to choose from a number of options minimising data input. Warnings to users upon submission of data to limit the uploading of personal data to what is strictly necessary in free text fields where personal data are likely to be included Staff of reporting authorities receive a side manual with warnings and guidance on data minimisation	2	1
2	Submission of personal data by reporting authorities	Corruption of data	Data quality, security	4	2	Measures to be agreed with reporting authorities: Changes are logged and backups kept Accuracy of data is first the responsibility of Reporting authorities uploading the information. They will be reminded every year to confirm data are still up to date. These verifications will apply to FSOs identifying natural persons and data listed in annex II of the RTS Quality control of the data submitted may also be performed by the AML/CFT team who is able to review the data submitted,	2	1

[19] This column describes technical details of the controls. AML and NF requirements listed here stand for functional and non-functional requirements as described in chapter 7(d)(4) of this DPIA

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
						ask for clarifications if needed and then approve/integrate the data Proactive info / reminder at stage of submission for limitation of data to be sent		
3	Submission of personal data by reporting authorities	Impersonation or data breach Security breach	Security	4	3	Measures to be agreed with reporting authorities in joint controllership arrangements: Limitation of access to those with need to know. Only Authorised / appointed users from reporting authorities will have access rights enabling submission of Material Weaknesses and related information / reasoned requests. Authorised/appointed users from reporting authorities will only be able to access data input by their AML/CFT reporting authority, i.e. cannot view data input by a different AML/CFT reporting authority. Protection of access to EBA system Accesses are logged and logs analysed. Monitoring and notification of unusual/unexpected attempts of access Database encrypted at rest and in transit Enforcing the EBA standard on access control rules, including multi-factor authentication. The joint controllership arrangement specifies that the parties shall provide each other with reasonable assistance as required to facilitate the handling of any data breach under the EUDPR, and that each party is responsible for personal data	2	2

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
						breaches that occur as a result of an infringement of that party's obligations.		
4	Possible feeding in from databases or platforms already controlled by the EBA	Sending of excessive/irrelevant data	Data quality	3	2	Limit where possible the processing to non-identifiable data Limit the processing of personal data. Note: in case there is in a future stage a connection with EUCLID, data concerned relate to legal persons, which only in rare case will identify natural persons.	1	1
5	Details of data processed by EBA: specific categories of data	Impact on fundamental rights of data subjects: risks to reputation of data subject and of exclusion from social/contractual benefits Data related to offences or suspicions of offences: Risk of starting judicial proceedings based on inaccurate information	Protection of special categories of data	4	3	Strict limitation of the processing of special categories of data. Quality control and safeguards at EBA level including control of the reliability of the information processed and annual reminders to reporting authorities to confirm that data are still relevant, accurate and up to date (e.g. when there is no definitive judicial decision against an individual) Automatic warning to users to limit the uploading of personal data to what is strictly necessary in relevant fields Specific safeguards in the interface developed for the transmission of data (see also above): Strict limitation of free text, breakdown of items for better formatting and preference for choosing from options	3	2

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
6	Analysis of data by EBA	Findings based on irrelevant, inaccurate or outdated information, with an impact on the reputation of individuals concerned and their possible exclusion from social/contractual benefits, as well as undue judicial proceedings against them	Necessity, proportionality, accuracy of data	5	3	The data submitted cannot be altered, but complemented with the submission by reporting authorities of a subsequent development. In case some deletion is needed, the AML/CFT Unit needs to create an IT request, duly documented and justified. Where relevant, classification of data according to their reliability: and manual re-assessment by EBA users. Periodic re-assessment of personal data classified as opinion and regular re-classification, if appropriate, of the data as fact (with reference to the appropriate sources) or alternatively the purging of such data. In the event of the data being retained verification and auditing is required. Use of data analytics techniques to perform regular data cleaning tasks to guarantee accurate results and prepare data for further analysis. When required the relevant inconsistencies will be clarified directly with the respective reporting authorities for accuracy. Decisions based on verified personal data	3	2
7	Analysis of data by EBA	Security breach	Security	4	2	*IT issues* Apply data classification in order to enhance protection of personal data Limitation of access to those with need to know. Only Authorised EBA users will have access to information submitted to EBA (data	2	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
						pertaining to all AML/CFT reporting authorities) Accesses are logged and logs analysed The database is encrypted at rest and in transit Data are stored on a server located in the EEA The joint controllership arrangement specifies that the parties shall provide each other with reasonable assistance as required to facilitate the handling of any data breach under the EUDPR, and that each party is responsible for personal data breaches that occur as a result of an infringement of that party's obligations.		
8	Sharing of data by EBA with reporting authorities, including ECB and SRB	Sharing of irrelevant or excessive information	Necessity and proportionality	4	3	By default, no personal data are shared by EBA, except if directly relevant for the analysis of AML/CFT case, via a reasoned request or on EBA initiative. Personal data are redacted where needed. In case of reasoned request of a reporting Authority concerning personal data: request of justification by reporting authority describing the necessity to process personal data (and why anonymised information is not sufficient)	2	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
						No personal data will be shared automatically. Sharing will be done manually, on a case-by-case basis, with a limitation of personal data to what is strictly needed. Personal data will be exported in a specific document (PDF/CSV/Excel files) supporting encryption and password protection.		
9	Sharing of data with judicial authorities	Sharing of irrelevant or excessive information Risk of starting judicial proceedings based on inaccurate information	Necessity and proportionality Processing of special categories of data	5	2	Additional quality control and safeguards at EBA level for data relating to suspicions of offences, including control of the reliability of the information processed	3	1
10	Sharing of data in context of close coordination with FIUs	Sending of inaccurate, excessive or irrelevant personal data, security breach, with possible impact on	Accuracy, necessity and proportionality Security	5	1	Sharing of data is operated outside of the platform. Very few cases of sharing are expected. Quality control and safeguards at EBA level including control of the reliability of the information processed and annual reminders to reporting authorities to confirm that data are still relevant, accurate and up to date.	3	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
		persons concerned				No personal data will be shared automatically. Sharing will be done manually, on a case-by-case basis, with a limitation of personal data to what is strictly needed. Personal data will be exported in a specific document (PDF/CSV/Excel files) supporting encryption and password protection. *Measures to be seen in context of broader cooperation with FIUs.*		
11	Sharing of data in context of institutional cooperation with EIOPA and ESMA	Sending of inaccurate, excessive or irrelevant personal data, security breach, with possible impact on persons concerned	Accuracy, necessity and proportionality Security	5	2	Sharing of data is operated outside of the platform. Quality control and safeguards at EBA level including control of the reliability of the information processed and annual reminders to reporting authorities to confirm that data are still relevant, accurate and up to date. No personal data will be shared automatically. Sharing will be done manually, on a case-by-case basis, with a limitation of personal data to what is strictly needed. Data are exported by EBA on its own initiative, or following a request received by these authorities providing reasons as to why that information is necessary for the achievement of their tasks (art 10(4)(e) RTS.	2	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
						Personal data will be exported in a specific document (PDF/CSV/Excel files) supporting encryption and password protection..		
12	System actors: contact persons within reporting authorities	Risk of outdated or incomplete list of persons entitled to access the interface, with a possible impact on the quality of the data and the security of the system	Accuracy, Transparency Security	3	2	Information for contact persons on the purpose of the processing of their data (contact details, credentials) and related security requirements Users accounts will be regularly reviewed. reporting authorities shall notify EBA if a user does not need access anymore. User password strength and updates should comply with EBA password policy	1	1
13	System actors: contact persons within EBA	Risk of outdated or incomplete list of persons entitled to access the database, with a possible impact on the quality of the data and the security of the system	Accuracy, Transparency Security	3	2	Information for EBA agents on the purpose of the processing of their data (contact details, credentials) and related security requirements Users accounts will be regularly reviewed. User password strength and updates should comply with EBA password policy	1	1
14	Data subjects rights	Incapacity for the data subject to properly	Rights of access, rectification, opposition, deletion	4	3	Clear identification in arrangements with co-controllers of respective responsibilities in terms of exercise of data subjects' rights, including the designation of a central	2	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
		exercise their rights				contact point for informing data subjects and allowing them to exercise their rights. *The arrangement specifies safeguards in case art 25 restrictions are adopted, limiting exercise of rights (e.g. in case disclosure would harm supervisory investigations)] EBA internal access procedure and role of delegated controllers to address individuals' requests, where needed in cooperation with concerned* reporting authorities[20]*. See in this respect EBA decision on conducting general searches of EBA systems*		
15	Cookies, plugins, IP address used in the interface for submission of data or reasoned requests	Processing of irrelevant or excessive data	Necessity and proportionality principles	2	2	Strict limitation of data collection (no third party cookies or plug-ins) Data used only for proper functioning and security of interface Information of users via a privacy policy notice available on the interface used for the submission of data	1	1

[20] As data subjects are entitled by law to exercise their rights in respect of and against each of the controllers (art 26.3 GDPR, art 28.3 EUDPR).

8. Data subject comments (if applicable)

The EBA is not in contact with data subjects as the collection of data is (will be) done indirectly via the actors mentioned above. Therefore, no specific consultation could take place.