Version 04/05/2021.The draft DPIA is not final and will be further complemented according to the RTS under article 9a (1) and (3)of the EBA Regulation and in parallel to the development of the database design.

6 May 2021

Summary of the draft Data Protection Impact Assessment on a central EBA database concerning anti money laundering and terrorist financing

Project name

1. Development of a Data Protection Impact Assessment (DPIA) for the establishment of a central database concerning anti money laundering and terrorist financing (AML/CFT) in fulfilment of the mandate conferred on the EBA under article 9a(1) and (3) of the EBA Regulation[1].

Review

2. A review of the data protection and privacy impacts of the central database is foreseen within a cycle of two years, starting when the system will be ready to enter into production. 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 interconnections with other databases, an extraordinary review of the DPIA will be performed.

Summary

Description of processing:

3. The EBA collects information from competent 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 competent authorities in response to these material weaknesses.

[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.

4. This information is centralised in a database controlled by the European Banking Authority in compliance with article 9a. (2) of EBA Regulation.

5. The data are analysed and shared, on a need to know and confidential basis, with competent 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 EBA Regulation. The data will be transmitted where relevant to national judicial authorities and the EPPO.

6. The central database operates in the wider context of close coordination between the EBA and other authorities at national and EU level. In that context, 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 FIUs pursuant to art 9a (1) (a) of EBA Regulation.

7. EBA determines together with the competent 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 possible 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 set out in Union or Member State law will therefore be specified in an arrangement[2].

Main findings of the DPIA

8. The purpose of the database foreseen in art 9a of the EBA Regulation is to process information on financial sector operators, which in most cases are not natural persons. 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

[2] 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 establishing 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. »

exclusion from social/contractual benefits and may also result in undue judicial proceedings against them.

9. For these reasons, controls and mitigation measures are foreseen, which

   - limit to the strict minimum the collection of identifiable information;
   - foresee a classification of personal data, independent from other sets of information, collected, triggering enhanced protection and safeguards, including their encryption, their redaction where relevant, and ad hoc retention periods.
   - secure the channels of communication with other authorities;
   - limit the sharing of identifiable data with other authorities and ensure that such sharing is operated manually (no automated sharing);
   - provide for additional quality and reliability controls for such information, especially where special categories of personal data such as data concerning criminal convictions and offences are concerned.

10. 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 competent authorities, and to the protection of sensitive data.

Reason for this DPIA

11. A DPIA is performed to assess the impact of the processing on the 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.

12. 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.

13. The processing aims at collecting data concerning financial operators which are in principle legal persons. As mentioned above, while individuals are not the main target of the processing, personal data will be included in the database (see chapter '*Analysis of risks and establishment of controls for identified risks*'). The following elements affect the assessment of the impact of the central database on individuals:

    - Data are collected from a large number of competent 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" (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[3].

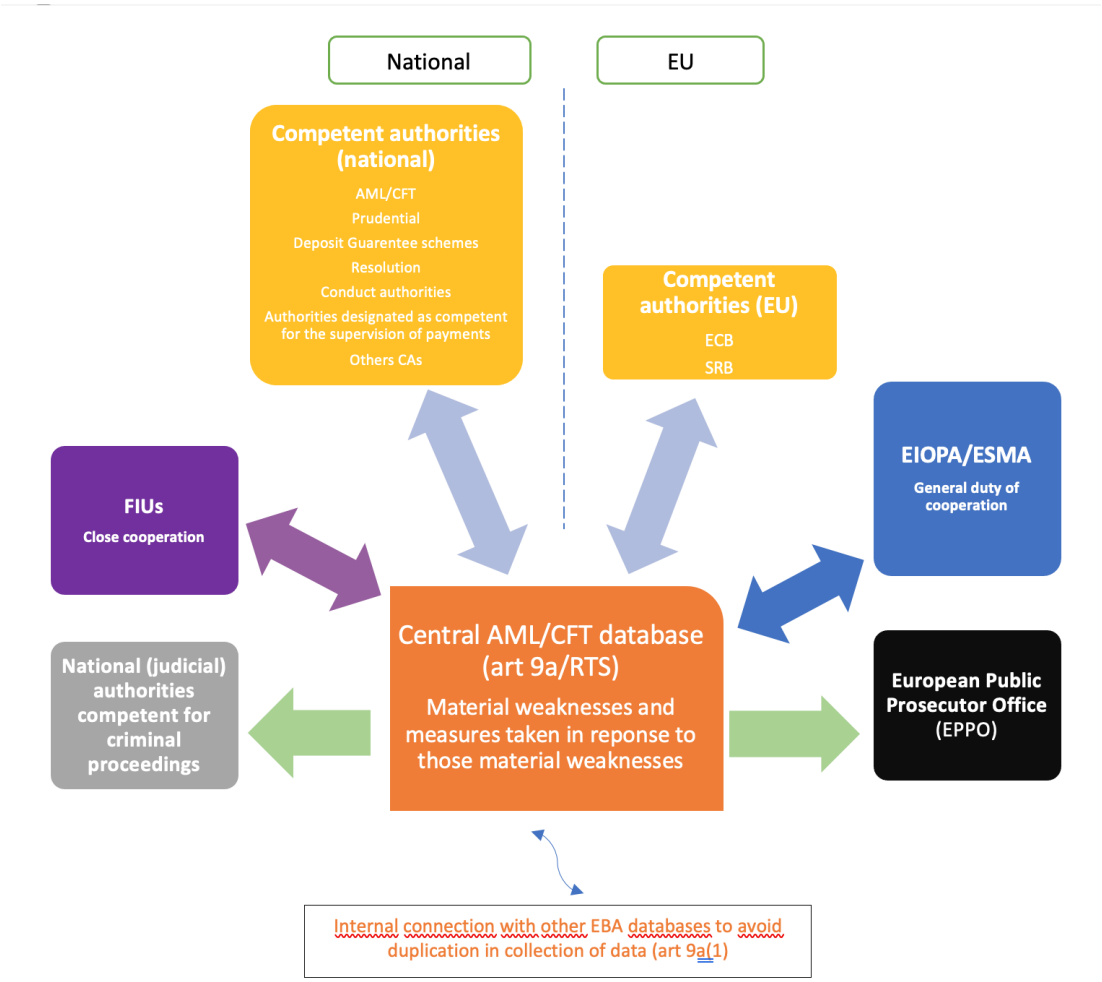
[3] Decision of the EDPS of 16 July 2019 on DPIA lists issued under articles 39 (4) and (5) of Regulation (EU) 2018/1725, available at https://edps.europa.eu/sites/edp/files/publication/19-07-16_edps_dpia_list_en.pdf

- 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, some data may likely be collected from existing databases or platforms already controlled by the EBA. This means that a matching or combination of data from different data sets may be considered.

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

Description of processing

Data flow diagram of the process (flowchart)



Source of the data

15. National and EU competent authorities as mentioned in article 9a 1(a) of EBA Regulation, and further detailed in article 3 of the Regulatory Technical Standards (RTS):

- authorities which identify weaknesses during their ongoing supervision and authorisation procedures, in the processes and procedures, governance arrangements, fitness and propriety, acquisition of qualifying holdings, business models and activities of financial sector operators as defined in Article 4 (1a) of Regulation (EU) No 1093/2010, in relation to preventing and countering money laundering and terrorist financing; and

- authorities, which take measures, in response to the material weaknesses affecting one or more requirements of the legislative acts referred to in Article 1(2) of Regulation (EU) 1093/2020, Article 1(2) of Regulation (EU) No 1094/2010[4] and Article 1(2) of Regulation (EU) No 1095/2010[5] and of any national laws transposing them with regard to the prevention, and countering the use of the financial system for the purpose, of money laundering or terrorist financing.

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

17. In practice, at national level, authorities listed in art 3 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

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

19. 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

[4] Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

[5] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

to the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

Categories of personal data

- 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 persons[6] in connection to the identification of material weaknesses[7], and measures taken in response to these weaknesses by competent authorities.

20. The data relate to several categories of persons:

- 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

[6] 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;"

[7] Under art 4 (1) of the drat Regulatory Technical Standards,
"For the purpose of point (a) of the first subparagraph of Article 9a of Regulation (EU) No 1093/2010 breaches, potential breaches and ineffective applications shall be weaknesses". Corresponding situations where weaknesses may occur are developed in annex 1 of the draft RTS.

Under art 5 of the draft Regulatory Technical Standards,

1. A weakness shall be considered material where it reveals or could lead to significant failures in the compliance of the firm, or of the group to which the firm belongs, with its AML/CFT requirements.
2. For the materiality of a weakness to be determined, all the following criteria shall be assessed:

(a) It occurs frequently;
(b) It has persisted over a significant period of time (duration);
(c) It is serious or egregious (gravity);
(d) The decision-making bodies of the firm either appear to have a knowledge of the weakness and decided not to remediate it or they adopted decisions or deliberations directed at generating the weakness (Negligence and wilful misconduct);
(e) The weakness increases the ML/TF risk exposure of the firm or the ML/TF risk associated with the firm, or of the group which it belongs to;
(f) The weakness has or could have a significant impact on the integrity, transparency and security of the financial system of a Member State or of the Union as a whole;

The weakness has or could have a significant impact on the viability of the firm or of the group to which the firm belongs to or on the financial stability of a Member State or of the Union as a whole;

[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

(customer or beneficial owner, member of the management body and key function holder in context of fitness and propriety assesment), when such legal and natural persons have a link with a material weakness.

- Measures taken in response to a material weakness:
  - Type of measure taken, in connection with a financial sector operator (if identifying a natural person) or an individual
  - Personal details: name(s), surname, function (checkboxes confirming whether the person is/was member of the management body)
- Implementation of the data collection within Competent authorities (CAs) and EBA:
  - CAs: name, position, and contact details 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, position and contact details of persons responsible for the reception, the processing and the sharing of information under the RTS.

21. General comment: *The purpose is to avoid identification of natural persons, and personal data are not expected in principle in the structured fields of the interface for the collection of data. They may be included in open 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 a client or a beneficial owner*[9], *member of management body or key function holder, with justification and specific safeguards. The data necessary to make sure the right person is identified may be collected: name, surname and date of birth, nationality, country of residence.*

Processing

22. 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.

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

24. Details of the processing:

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).

- Collection of data on material weaknesses from competent authorities. Data are pushed manually[10] by competent authorities to the EBA via an interface set up by the EBA. Data are also collected from existing databases as developed in c. below.
- Centralisation of the data in the EBA AML/CFT database foreseen in art 9a(2) of EBA Regulation
- Analysis of the data collected, using analytic third party tools when required, with the purpose of examining material weaknesses and measures taken in response to these weaknesses, as described in b. below, validating compliance data on natural and legal persons (ex: Beneficial Owner structures) as well as, where needed, complementing the collected information with details not available in the submission (ex: adverse media, sanctions data).
- Sharing of data on a case-by-case basis with competent authorities, with FIUs in the context of close coordination with the EBA, with 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 competent 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).

Storage

25. Data will be stored and processed by the EBA exclusively within the EEA, as developed in the chapter 'Description of the supporting infrastructure' below.

26. Data will be kept in an identifiable form in principle for a period of ten years. At the end of that 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 necessity of the data on a case-by case-basis will be performed on a yearly basis, based on the systematic classification and categorisation of data and their date of collection. Depending on the volume of data, the assessment of the necessity to store them further or to delete them will be done manually or in an automated way.

27. The retention period of 10 years 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.

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

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

29. The retention period of reference of 10 years will be reassessed and adapted if it proves excessive or insufficient. The evaluation exercise will take place at the end of the 10-year period, and if it is concluded that this period is not adapted, the estimation of the actual retention time needed (reduced or extended) will be justified. This approach is similar as the one applied in AML context by the EIB after consultation of the EDPS[11], and also as currently discussed for the sanctions database controlled by the EBA.

Sharing of data

30. The data are shared with competent authorities:

- on a need to know and confidential basis, based on a reasoned request of the competent 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 competent authorities on a case-by-case basis.

31. Recipients of the data:

- EU entities
    - EU competent authorities
        - SRB
        - ECB
    - 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 are shared with these institutions and bodies in compliance with existing Regulations, protocols or MoUs framing the conditions of the sharing of data and related security and confidentiality safeguards.

- Other recipients within the EU

[11] Opinion of the EDPS on a notification for Prior Checking received from the Data Protection Officer of the European Investment Bank regarding AML-CFT data processing, point 3.5, p. 11

- National competent authorities under art 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 (art 9a (1). a et b. EBA Regulation)

- National judicial authorities and other competent authorities when information could give rise to criminal proceedings in accordance with national procedural rules (Art 9a (2) of EBA Regulation).

Detailed description of the purpose(s) of the processing

32. 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.

33. 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.

Description of interactions with other processes

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

34. Personal data will be fed in from existing systems handled by authorities competent for AML/CFT at national and EU level listed in 7.a.

35. To avoid duplication of data collection as provided in art 9a(1) EBA Regulation[12], some data may be fed in from databases or platforms already controlled by the EBA, for instance applications using the e-gate portal, as long as these data are already being processed for the purpose of AML/CFT.

Re-use of personal data in other processes

36. Data will be made available to competent authorities on a need-to-know and confidential basis and transmitted where relevant to national judicial authorities and the EPPO.

37. As mentioned in 4. above, the process will also result in interactions and sharing of data with EIOPA and ESMA as part of the general duty of cooperation foreseen in article 2(4) of EBA Regulation and with FIUs pursuant to art 9a (1) b. of EBA Regulation.

38. 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.

39. 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.

Description of the supporting infrastructure: filing systems, ICT etc

40. The infrastructure is not yet defined at this stage of the development of the project.

41. Confidentiality, integrity and availability requirements will be implemented in the Information Security Risk Management for all stages of data processing.

42. In practice and considering the current development of the IT system, the following can already be mentioned:

43. Information will only be processed on a need-to-know basis.

- For the collection of information, the objective is to have an interface to be used by contact persons identified in each competent authority, with a strictly defined structure including predetermined fields for the users to feed in the database.
- The interface will be fed in manually by the users.
- Open fields will be limited to a minimum, and warnings will be set to automatically inform users on the limitation of uploading of personal data to what is strictly required, and to the applicable security safeguards.

44. With regard to the maintenance and operation of the central database by the EBA, the database will be hosted within the EEA, and the database will be subject to strict security measures, such as encryption, monitoring and multi-factor authentication.

[12] "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".

45. Data will not be shared with authorised recipients in an automated way. Sharing of personal data will be assessed on a case-by-case basis and will be operated manually.

Necessity and proportionality

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

46. Personal data are in limited cases necessary for the analysis of weaknesses as foreseen in art. 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;
- Measures taken by a competent 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.

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

47. 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. Art 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[13].
- 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).

[13] « 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 operator concerned, the reason for the information request as well as whether the information has been shared »

48. 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.

Analysis of risks and establishment of controls for identified risks

Introduction to the methodology

49. The table on the next pages analyses the risks and lists the controls that will be established for the identified risks.

50. 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.

51. The numbers suggested in the columns of this table 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 CAs (compared to EBA), because of the number of CAs 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	Severity (residual)	Likelihood (residual)
1	Submission of personal data by competent 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. Automatic warning to users to limit the uploading of personal data to what is strictly necessary Staff of competent authorities receive a side manual with warnings and guidance on data minimisation	2	1
2	Submission of personal data by competent authorities	Corruption of data	Data quality, security	4	2	Measures to be agreed with competent authorities: Changes are logged and backups kept Proactive info / reminder at stage of submission for limitation of data to be sent	2	1
3	Submission of personal data by competent authorities	Impersonation or data breach Security breach	Security	4	3	Measures to be agreed with competent authorities: Limitation of access to those with need to know. Only Authorised / appointed users from CAs will have access rights enabling submission of Material	2	2

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
						Weaknesses and related information / reasoned requests. Authorised/appointed users from CAs will only be able to access data input by their AML/CFT CA, i.e. cannot view data input by a different AML/CFT CA Protection of access to EBA system Accesses are logged and logs analysed Data is encrypted at rest and in transit Enforcing the EBA standard on access control rules, including multi-factor authentication.		
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	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	Protection of special categories of data	4	3	Strict limitation of the processing of special categories of data. Additional quality control and safeguards at EBA level for data relating to suspicions of offences, including control of the reliability of the information processed (e.g. when there is no definitive judicial decision against an individual)	3	2

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
		exclusion from social/contractual benefits Data related to offences or suspicions of offences: Risk of starting judicial proceedings based on inaccurate information				Automatic warning to users to limit the uploading of personal data to what is strictly necessary and specific alert for special categories of data 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 Masking/ encryption of personal data		
6	Analysis of data by EBA	Findings based on irrelevant, inaccurate or outdated information, with an impact on the reputation of individuals	Necessity, proportionality, accuracy of data	5	3	Verification of data accuracy Classification of data according to their reliability: 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.	3	2

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
		concerned and their possible exclusion from social/contractual benefits, as well as undue judicial proceedings against them				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 CAs for accuracy. Decisions based on verified personal data		
7	Analysis of data by EBA	Third party tools processing going beyond legal scope of the database (transfer of data outside the EU), risk of unlawful access to data (unlawful re-	Accuracy, purpose limitation, Transparency Security	4	1	Review by EBA of third party privacy policy, which should include guarantee that data processed strictly under purpose identified, and analyse issue of possible transfer outside EU; Identification and assessment of sub-processors (if any) and their location; Review of measures put in place by the provider(s) to ensure the safety of data.	2	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
		use, security breach)						
8	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 pertaining to all AML/CFT CAs) Accesses are logged and logs analysed Data are encrypted Data are stored on a server located in the EU	2	1
9	Sharing of data by EBA with competent authorities	Sharing of irrelevant or excessive information	Necessity and proportionality	4	3	By default, no personal data are shared by EBA (data are anonymised), except if directly relevant for the analysis of the AML/CFT case In case of reasoned request of a Competent Authority concerning personal data: request of justification by CA describing the necessity to process personal data (and why anonymised information is not sufficient) No personal data will be shared automatically. Sharing will be done manually	2	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
10	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
11	Sharing of data in context of close coordination with FIUs					*To be addressed in context of broader cooperation with FIUs*		
12	Sharing of data in context of institutional cooperation with EIOPA and ESMA					*To be addressed in context of broader cooperation with EIOPA and ESMA*		

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
13	System actors: contact persons within CAs	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	1	1
14	System actors: contact persons within EBA	Risk of outdated or incomplete list of persons entitled to access the database, with a possible impact on	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	1	1

Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity	Likelihood	Controls	Severity (residual)	Likelihood (residual)
		the quality of the data and the security of the system						
15	Data subjects rights	Incapacity for the data subject to properly exercise their rights	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 identification of controller(s) responsible for informing data subjects on contact point and procedure to exercise their rights.	2	1
16	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

Data Subject comments

52. 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.