FINANCIAL INTELLIGENCE ANALYSIS UNIT

CONSULTATION DOCUMENT

WWW.FIUMALTA.ORG

Consultation Process with Credit and Financial Institutions on the Draft Regulations providing for the Establishment of an Automated Centralised Mechanism for the Collection and Retrieval of Data on Bank Accounts, Payment Accounts and Safe Custody Services

ISSUED ON 26 MAY 2020

CONSULTATION CLOSING ON 12 JUNE 2020

Introduction

One of the amendments carried out by Directive (EU) 2018/843 was the introduction in Directive (EU) 2015/849 of the new Article 32a. This provision obliges Member States to establish centralised automated mechanisms for the collection and retrieval of data on bank and payment accounts as well as on safe custody services provided by credit institutions.

As a minimum, any such data has to be accessible to Financial Intelligence Units and other national competent authorities where this is necessary for the carrying out of their functions under Directive (EU) 2015/849. In addition, Directive (EU) 2019/1153 obliges Member States to widen access to these centralised automated mechanisms so as to allow the data retrievable through the same to be also accessible by national competent authorities for the prevention, detection, investigation and prosecution of serious criminal offences.

Issue of Consultation Document

Act I of 2020 designated the Financial Intelligence Analysis Unit ("FIAU") as the authority responsible for the establishment, management and administration of Malta's automated centralised mechanism. Subsidiary legislation is to be issued under the Prevention of Money Laundering Act ("PMLA") to complement the new paragraph (n) under Article 16(1) of the PMLA, setting out in more detail how this mechanism is to be established, managed and controlled by the FIAU. A first draft of the regulations to be issued under the PMLA is being published today for consultation with interested parties.

These draft regulations seek to achieve the following:

a. Identify the subject persons that will have to report data through this mechanism as well as setting out in general terms the data that these subject persons will have to report and the circumstances where this obligation will be triggered;

b. The obligations and powers of the FIAU in establishing, managing and administering this mechanism; and

c. Identify the authorities which will be granted access to the data retrievable through this mechanism and the conditions which they will have to meet to be allowed access thereto, as well as the circumstances where they are allowed to make use of any such data.

The FIAU is inviting all credit and financial institutions to provide their feedback on the proposed regulations. To the extent possible, feedback should be channeled through the representative bodies sitting on the Joint Committee for the Prevention of Money Laundering and the Funding of Terrorism.

Where this is not possible, subject persons may correspond directly with the FIAU using the following email address: consultation@fiumalta.org .

Feedback on the draft regulations should reach the FIAU **by not later than Friday, 12 June 2020**.

Centralised Bank Account Register Regulations

1. (1) The title of these regulations is the Centralised Bank Account Register Regulations.

(2) The objective of these regulations, issued in terms of Article 12(3) of the Prevention of Money Laundering Act, is to implement the provisions of Directive(EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 and of Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 relative to centralised automated mechanisms allowing for the identification, in a timely manner, of any natural or legal persons holding or controlling payment accounts and bank accounts identified by IBAN, or making use of safe custody services provided by credit institutions.

2. (1) In these regulations, unless the context otherwise requires:

"Act" means the Prevention of Money Laundering Act;

"beneficial owner" shall have the meaning assigned to it under the Prevention of Money Laundering and Funding of Terrorism Regulations;

"credit institution" means any one of the following:

(a) a person or institution who is for the time being licensed under the provisions of the Banking Act;
(b) a branch in Malta of any person or institution who has been granted an equivalent licence or authorization under the laws of any other jurisdiction; and
(c) the Central Bank of Malta;

"customer" shall have the meaning assigned to it under the Prevention of Money Laundering and Funding of Terrorism Regulations;

"financial institution" means any one of the following:

(a) a person or institution who is for the time being licensed under the provisions of the Financial Institution Act; and

(b) a branch in Malta of any person or institution who has been granted an equivalent licence or authorization under the laws of any other jurisdiction;

"IBAN" means an international payment account number identifier, which unambiguously identifies an individual payment account, the elements of which are specified by the International Organisation for Standardisation;

"safe custody" means the holding of tangible assets on behalf of customers;

"serious criminal offences" means tax evasion, an offence under the National Interest (Enabling Powers) Act and any other offence listed in Annex I to Regulation (EU) 2016/794;

"register" means the centralised automated mechanism referred to in Article 16(1)(n) of the Act.

(2) Words and expressions used in these regulations which are also used in the Act shall have

the same meaning assigned to them in the Act.

3. (1) Where a credit or financial institution provides an account identified by IBAN, or where a credit institution provides safe custody services, the credit or financial institution shall, for the purposes of these Regulations, maintain an electronic record of such data and information as may be prescribed by the Unit in relation to the following:

(a) the customer and, where applicable,
   i. Any agent thereof authorized to act on the customer's behalf; and
   ii. The beneficial owner of the customer;

(b) the IBAN associated with any such account or the alphanumeric code used to identify safe deposit boxes or any items entrusted to a credit institution when providing any safe custody services as are referred to hereabove;

(c) the length of time for which any account or safe custody services are provided as set out hereabove; and

(d) any other data or information on bank or payment accounts or safe custody services provided by credit institutions as the Unit may set out from time to time in procedures issued under regulation 5.

(2) Credit and financial institutions shall ensure that any data that they may be required to hold in terms of sub-regulation (1) hereabove is at all times adequate, accurate and up to date, and the electronic record thereof shall be updated immediately upon the credit or financial institution being informed or otherwise becoming aware that any of the data or information required to be held has changed.

(3) Regulation 13 of the Prevention of Money Laundering and Funding of Terrorism Regulations, shall be equally applicable to the retention of the data and information that credit and financial institutions may be required to hold in terms of sub-regulation (1) hereabove.

4. (1) The Unit shall establish, manage and administer the register wherein there shall be retained data and information on accounts identified by IBAN held by credit and financial institutions and on safe custody services provided by credit institutions, which data and information is to allow for the timely identification of any person or persons holding or controlling any such accounts or assets held under safe custody, or who may have held or controlled any such accounts or assets.

(2) The register shall contain an electronic record of the data and information that credit and financial institutions are required to hold in terms of regulation 3(1), which data and information is to be made available by credit and financial institutions in such format and with such frequency as may be prescribed by the Unit.

(3) In carrying out the functions referred to in regulation 3(1) hereabove, the Unit shall have regard to the highest technological standards and shall ensure that any of its officers or employees responsible for its management and administration are of high integrity and receive proper and regular training as to the confidentiality and data protection obligations applicable to the register.

(4) Any data or information contained in the register shall be so held for five years following the closure of the account or the termination of the safe custody service as may be applicable, upon the expiry of which the data and information so held shall be deleted:

Provided that the period of five years may be further extended, up to a maximum retention period of ten years, where such extension would be considered necessary for the purposes of the prevention, detection, analysis, investigation or prosecution of money laundering, associated predicate offences, funding of terrorism or any other serious criminal offence.

(5) The rights of the data subject referred to in regulation 4 of the Restriction of the Data Protection (Obligations and Rights) Regulations, in particular the right of access, shall be restricted, partially or completely, where such a restriction is necessary and proportionate for the Unit to ensure the proper functioning of the register.

5. The Unit may issue procedures and guidance as may be necessary for the purpose of prescribing anything required under these regulations and to ensure the proper functioning of the register, with any such procedures being binding on credit and financial institutions.

6. (1) The data and information held in the register shall be accessible, in line with procedures set out by the Unit, by the following authorities:

(a) the Unit;
(b) national authorities conducting criminal investigations into or prosecutions of money laundering, associated predicate offences, funding of terrorism or any other serious criminal offence, including when supporting investigations concerning any of the said offences;
(c) the Asset Recovery Bureau;
(d) the Commissioner for Revenue;
(e) the Sanctions Monitoring Board; and
(f) the Security Service.

(2) Each of the authorities listed in sub-regulation (1) shall access and make use of the data and information contained in the register on a case-by-case basis and to the extent that this may be necessary for the prevention, detection, investigation or prosecution of money laundering, associated predicate offences funding of terrorism or any other serious criminal offence, and for the avoidance of any doubt this shall include supporting investigations concerning any such offence, including the identification, tracing and freezing of the assets related to such investigation.

Provided that the above shall be without prejudice to any access to data and information held in the register that the Unit may require for the proper carrying out of its functions under regulation 4(1) hereabove.

(3) In addition to the access referred to in sub-regulation (2) hereabove, the data and information contained in the register may also be used to produce such aggregate or statistical data as may be required by the authorities referred to hereabove for the same purposes as are referred to in sub-regulation (2) hereabove.

(4) The authorities listed in sub-regulation (1) may also access and make use of the data and information contained in the register to reply to justified requests for information received

from foreign or supranational bodies having similar functions upon ascertaining that the requesting body applies confidentiality and data protection requirements equivalent to those applicable to them;

Provided that such authorities shall be required to disclose on behalf of which authority the disclosure is being effected.

(5) Each of the authorities listed in sub-regulation (1) shall designate one or more of their officers or employees that are to have access to and carry out searches in the register, with each designated officer or employee being granted the said rights only upon undergoing such registration or accreditation process as may be established by the Unit.

(6) The authorities listed in sub-regulation (1) above shall implement the necessary safeguards to ensure that data and information held in the register is accessed and made use of only when this is strictly required for the purposes set out in sub-regulation (2) hereabove.

(7) In meeting their obligation under sub-regulation (6) hereabove, and having due regard to the sensitivity of the data and information involved, the authorities listed in sub-regulation (1) shall, as a minimum:

(a) ensure that they maintain high professional standards of confidentiality and adherence with the applicable data protection requirements, including through monitoring compliance with the said standards, and that all of their officers and employees are of high integrity;

(b) provide any officer or employee designated in terms of sub-regulation (5) hereabove, or any officer or employee able to request any such employee to carry out searches in the register, with the necessary training on how to handle data and information accessible through the register in line with data protection requirements;

(c) establish internal policies and procedures setting out the conditions and circumstances in which data and information is to be obtained from the register, including safeguards to avoid unauthorized or unjustified access thereto, and monitoring the application of the same;

(d) apply technical and organisational measures to ensure the security of the data to high technological standards; and

(e) ensurie that the Unit is promptly informed whenever an officer or employee is no longer to be considered as a designated employee in terms of sub-regulation (5) above.

(8) Where any of the authorities become aware that the data or information held in the register is not correct or is otherwise not up to date, the authority concerned shall immediately inform the Unit.

(9) Each authority listed in sub-regulation (1) shall hold statistical data on the number of searches carried out through the register and shall make the same available to the Unit or to the European Commission upon request or in line with such procedures as may be established.

7. (1) The Unit shall establish such procedures as it may deem proper to monitor and regulate the access and the carrying out of searches for data and information contained in the register, which procedures shall include the retention of the following information with respect to each search:

(a) the case reference number;
(b) the date and time of the query or search;
(c) the type of data used to launch the query or search;
(d) the unique identifier of the results;
(e) the name of the authority consulting the registry;
(f) the unique user identifier of the designated officer or employee referred to in regulation 6(5) above and, where applicable, of the official who ordered the query or search and, as far as possible, the unique user identifier of the recipient of the results of the query or search.

(2) The information referred to in paragraphs (a) to (f) above shall be:

(a) held only to monitor confidentiality and data protection requirements, including checking the admissibility of a request and the lawfulness of data processing, and for ensuring data security;
(b) accessible only to the data protection officer of the Unit, who shall check the same on a regular basis, and, upon request, to the Information and Data Protection Commissioner; and
(c) protected by appropriate measures against unauthorised access and shall be erased five years after its creation, unless it is required for monitoring procedures that are ongoing.

(3) In the event that the authorities listed in regulation 6(1) become aware of any unauthorized or unjustified access to the register, they shall promptly inform the Unit and provide it with any information in relation to any such unauthorized or unjustified access as may be requested by the Unit.

(4) The Unit may, where it considers that any of the authorities are not implementing the necessary safeguards to prevent unauthorized or unjustified access to the register and to the date and information contained therein, or are otherwise failing to comply with any of their obligations under these Regulations, terminate the authority's access and only provide the same again once the authority has implemented the necessary measures to prevent the same from occurring again.

8. (1) The Unit shall be responsible to monitor that credit and financial institutions meet their obligations under these regulations and any procedures and guidance issued under regulation 5 hereabove.

(2) For the purposes of carrying out its functions under sub-regulation (1), the Unit may exercise any of the powers granted to it under Article 26 of the Act as well as carry out data quality checks on the data and information provided by credit and financial institution for inclusion in the register as it may deem fit and give such directions as may be necessary to redress any issues identified with respect to such data and information.

(3) In accordance with Article 13 of the Act, any credit or financial institution who contravenes

any provision of these regulations or of any procedure or guidance issued in terms of regulation 5 hereabove as well as any direction given by the Unit shall be liable to an administrative penalty of not less than two hundred fifty Euro (€250) and not more than forty-six thousand five hundred Euro (€46,500) in respect of every separate breach:

(4) Notwithstanding the provisions of sub-regulation (3), the Unit may:

(a) with respect to minor contraventions and where the circumstances so warrant, impose an administrative penalty below the minimum established by these regulations but not less than two hundred and fifty Euro (€250) or issue a reprimand in writing instead of an administrative penalty;

(b) with respect to serious, repeated or systematic contraventions, impose administrative sanctions that in total are not to exceed Euro one million (€1,000,000);

(c) instead of or in conjunction with the imposition of any administrative penalty as envisaged under this regulation, require the credit or financial institution to take any action or measure to remedy such contravention or to ensure compliance with the provisions of these regulations or any procedures issued by the Unit.

(5) Administrative measures under these regulations shall be imposed by the Unit without recourse to a court hearing and in accordance with policies and procedures established by the Board of Governors referred to in the Act, with the Unit being able to impose penalties either as a one-time fixed penalty or as a daily cumulative penalty or both:

Provided that an administrative penalty imposed on a daily cumulative basis shall not be less than two hundred and fifty (€250) and the accumulated penalty shall not exceed the maximum set out under sub-regulations (3) and (4)(b) as may be applicable.

(6) Article 13A to Article 13C of the Act shall be equally applicable in relation to any administrative measure imposed on a credit or financial institution for any contravention of these regulations or of any procedures or guidance issued in terms of regulation 5 hereabove.