Project Number 683612

D 8.2 – Final Report on specifics for Global European market entry

Version 1.6
08 July 2016
Final

Public Distribution

petaFuel

Project Partner Contact Information

petaFuel GmbH
Ludwig Adam
Muenchnerstrasse 4
85354 Freising
Germany
Tel: +49 8161 40 60 202
E-Mail: ludwig.adam@petafuel.de

Table of Content

Document Control

Version	Status	Date
1.0	Document outline	27 June 2016
1.1	Initial Document Draft	29 June 2016
1.2	First Document Draft	30 June 2016
1.3	Second Document Draft	05 July 2016
1.4	Initial Final Draft	06 July 2016
1.5	Final	07 July 2016
1.6	Amended Final	08 July 2016

Executive Summary

This document constitutes deliverable *D 8.2 – Final Report on specifics for a global European market entry* of Work Package 8 (WP8) of the VIMpay project.

The deliverable details the regulative and technical requirements and specifics in Europe for the global adoption of the VIMpay solution in the SEPA region of Europe.

Also documented are the specific regulative and technical aspects in relation to the potential risks involved when globally adopting VIMpay in other European countries and alternative solutions that potentially might be needed should the need arise.

1 Introduction

VIMpay is proving to be a successful solution that warrants expansion into the EU. For the expansion to be seamless and cost-effective, certain requirements regarding the complete European market entry need to be satisfied in order to avoid costly delays or potential redesigns on the path to global marketization.

Alignment of the existing technical and regulatory frameworks in Europe is being taken into account for the global marketization of VIMpay in Europe. For the VIMpay global European market entry strategic path, proposed and upcoming regulations have also been accounted for.

2 Global Focus on Single Euro Payments Area (SEPA)

petaFuel´s existing payment infrastructure is fully compliant with all SEPA payment schemes which positively positions VIMpay within the SEPA payments realm. On the other hand, PayCenter will facilitate SEPA payments by issuing to all VIMpay customers a SEPA-compliant payment account that is capable of SEPA Credit Transfers (SEPA SCT) payments and allow incoming SEPA Direct Debits (SEPA SDDs).

The advantage here is that petaFuel can generate and process all incoming and outgoing SEPA payments of these PayCenter issued accounts. Due to the inherent payment risks, VIMpay will not offer outgoing SEPA Direct Debits (SEPA SDDs) services to merchants.

The EPC (European Payment Council) has been working for the last 6 years with the relevant players in the mobile money space to create a secure and stable system that will enable the initiation and receipt of SEPA payments by mobile phone. The EPC and GSM (Global System for Mobile Communications) have been laying the foundation for implementing Mobile Contactless Payments (MCP) which fits in well with the VIMpay Pan-European business case.

VIMpay SEPA payments have been made easier as well with the ERPB's (Euro Retail Payments Board, formerly the SEPA Council) decision to review the post-migration issues relating to SEPA credit transfers and SEPA direct debits. Additionally, the review of the Pan-European electronic mandates for SEPA direct debits will assist VIMpay with its transition into a functional Pan-European solution.

3 VIMpay Objectives

As previously mentioned in deliverable D 4.1 Decision Matrix and Process Definitions of Work Package 4 (WP4) and deliverable D 8.1 Report on European Focus Countries of Work Package 8 (WP8), VIMpay card payments and account issuing are the two primary objectives that needed review and clarification. A Pan-European entry requires a stable and uninterrupted framework which is present in the case of VIMpay.

3.1 VIMpay Card Payments

VIMpay benefits from a proven and well-established card-based payment infrastructure. Card payments are critical to the VIMpay value proposition and having a card issuer already connected to petaFuel's processing infrastructure is paramount to a successful Pan-European market entry. petaFuel will process VIMpay payments between all 36 mllion merchants with MasterCard acceptance worldwide and the issuing financial institution PayCenter.

PayCenter as the card issuer

PayCenter is a licensed and preferred MasterCard issuer. It focuses primarily on the prepaid card business, especially prepaid MasterCards. Issuing of the VIMpay Card, which is a MasterCard will be done by PayCenter because of the existing partnership.

PayCenter currently holds the following card issuing license:

MasterCard EEA Issuing License

The MasterCard EEA issuing licence allows PayCenter to issue VIMpay Card as a MasterCard-branded Pan-European payment card.

3.2 VIMpay Account Issuing

As described in D7.1 - First enhanced exploitation and pricing plan and D7.2 Final exploitation plan, a uniform exploitation strategy will be employed for Germany and for the whole of the EU. The ideal VIMpay customer parameters and the Freemium pricing strategy revolves aropund the ability to effectively issue accounts.

PayCenter as the account issuer

The most effective VIMpay account issuing option for the EU is using PayCenter as the issuer because of the established licensing availability. PayCenter was the first German eMoney Institute with its own German bank code to be approved and licensed by the Federal Financial Supervisory Authority (BaFin).

PayCenter currently holds the following account issuing license:

E-Money License issued by the Federal Financial Supervisory Authority (BaFin)

With the BaFin E-Money licence, PayCenter is able to operate within the “passporting procedure” in all other EU countries.

4 Third Party Account Access

Account access for third parties is one of the core features of VIMpay. It essentially facilitates multi-banking in other European jurisdictions. As mentioned in deliverable D 8.1 Report on European Focus Countries of Work Package 8 (WP8), HBCI/FinTS or Home Banking Computer Interface/ Financial Transaction Services is the unified protocol used by German banks.

FinTS (Financial Transaction Services), the successor of the HBCI, is adopted in Germany because it is a modern and secure transmission method for online payments, HBCI allows bank customers to perform home banking transactions through a standardized interface between customers and the bank server software.

For a VIMpay European market entry, petFuel has settled for a pair of alternatives to the HBCI/FinTS protocol in order to ensure VIMpay offer multi-banking services in the whole of Europe.

4.1 Technical Strategy as described in D 8.1

As decribed in deliverable D8.1, the most vital functionality that could present technical challenges for the adoption and integration of VIMpay in the EU is multi-banking. VIMpay will allow its users to access third party banks. However, due to the presence of varying multi-banking protocols, petaFuel has had to choose two (2) protocol that are uniform across the EU.

4.1.1 Banking Application Programming Interfaces (APIs)

Some European banks directly provide interfaces to connect with their internal systems. petaFuel will leverage these interfaces to facilitate multi-banking for the VIMpay users. In contrast to standardized protocols, APIs are often bank-specific and must be implemented individually per bank system. For European banks offering an API, VIMpay will seamlessly be able to facilitate Multi-banking.

4.1.2 Screenscraping

Screen scraping is the process of collecting screen display data from one application and translating it so that another application can display it. This is normally done to capture data from a bank application/web interface in order to display it using a third party application. For the European countries with existing protocols that require costly adjustments, Screenscraping will be a viable option for VIMpay to access third-party account in order to facilitate multi-banking capabilities.

4.2 Impact of Payment Services Directive II (PSD II) on third party access

The Payment Services Directive II (PSD II) was formally adopted by EU law makers in November 2015. The directive will need to be implemented into national legislation across the 28 EU countries and the rules come fully into effect from the 13th of January 2018.

4.2.1 Secure access to payment account

The key elements of PSD II that have the most impact on VIMpay include the opening of access across the banking industry to payment processing services, as well as to the customer accounts held by banks. The directive recognizes a growing market demand for payment service providers (PSPs) granting third parties access to their online payment services in a regulated and secure way. This is the Third Party Payment (TPP) service provision in the directive's terminology.

Additionally, the 'Access to Accounts' (XS2A) rule will force banks to facilitate access via an API to their customer accounts and provide account information to third party apps such as VIMpay if the account

holder wishes to do so. This is a positively critical aspect of the directive that allows VIMpay to globally offer multi-banking capabilities across Europe.

4.2.2 Proposed EBA framework/protocol (currently under development)

The final shape of the PSD II is still under review. The EBA (European Banking Authority) is currently working to set standards and, critically, the national implementation process will add a great deal more guidance around how PSD II will be applied.

The EBA has a role, under PSD2, to draft a range of technical and regulatory standards which will set out in more detail how petaFuel and VIMpay, subject to PSD II, can comply with the rules set within the Directive.

A proposed EBA rule will involve "trusted beneficiaries". petaFuel could be able to sanction low-value VIMpay payments, VIMpay payments made to "trusted beneficiaries" and the VIMpay transfer of funds between different payment accounts that a VIMpay account holder has, without having to complete a multi-factor authentication process under the proposed new EU payment services rules.

5 "Know Your Customer" (KYC)

As previously clarified in deliverable D 4.1 Decision Matrix and Process Definitions of Work Package 4 (WP4) and deliverable D 8.1 Report on European Focus Countries of Work Package 8 (WP8), the KYC models below form the overall VIMpay KYC structure and ongoing customer due diligence processes.

VIMpay Decision Matrix							
Basic VIMpay KYC Structure							
VIMpay Version	**Preset KYC Model**	**Instant top-up limit**	**Maximum Account Balance**	**Revenue Limit per year**	**KYC Requirements**	**VIMpay Functionalities**	**Additional Requirements**
NOT CURRENTLY SUPPORTED	NO KYC Anonymous	15€	100€	100€	None	"Gift card" with limited use only	
						Reloading the card for the second time	Basic Small KYC
Standard	Small KYC	15€	300€	2,500€	1. Reference bank account 2. Mobile phone number verification via TAN 3. Automatic address check	1. Mobile phone recharge 2. Account recharge via Instant Replenishment 3. ATM Cash withdrawals 4. Internet purchases 5. POS purchases	
						6. Plastic VIMpay card and ATM withdrawals	Basic Small KYC + Address verification / Proof of address in the form of a residence registration certificate before the plastic card is sent
Plus Upgrade	Small KYC	150€	2,500€	2,500€	1. Reference bank account (NOT required if upgrading from VIMpay standard and a Small KYC check is already accomplished) 2. Mobile phone number verification via TAN 3. Automatic address check	1. Mobile phone recharge 2. Account recharge via instant replenishment 3. Account recharge via a bank transfer 4. ATM Cash withdrawals 5. Internet purchases 6. POS purchases	
						7. Plastic VIMpay card and ATM Cash withdrawals	Basic Small KYC + Address verification/Proof of address in the form of a residence registration certificate before the plastic card is sent

Premium Upgrade	Full KYC	Unlimited	10,000€	Unlimited	1. PostIdent / VideoIdent 2. Mobile phone number verification via TAN	1. Plastic VIMpay card and ATM Cash withdrawals 2. Internet purchases 3. POS purchases 4. Mobile phone recharge 5. P2P payments (among VIMpay users) 6. Bank transfers (SEPA) 7. Bank account functionalities 8. BankingBro 9. Recharge via Instant replenishment 10. Recharge via a normal bank account	
						11. Increasing the maximum account balance above the 10.000 € limit	Basic Full KYC + A telephone call to the VIMpay customer service number to review the customer account

5.1 Small KYC

For the VIMpay Basic version, the Small KYC will be required in Germany and the rest of Europe. Key to this model will be the need for a user reference bank account. Additionally, a mobile phone number verification via TAN and an automatic address check will be conducted.
As mentioned in D4.1 Decision matrix and process definitions, all VIMpay Small KYC processes have been defined and adopted with a view of the wider EU market entry in mind and the ease of process adaption in the EU without jeopardizing other project efforts.

Reference Account

In accordance to the most current BaFin ruling, a reference bank account is critical during account opening, especially for E-Money institutions. As illustrated in the above table, a reference account will be required as part of the VIMpay Small KYC model for the whole of Europe.

The process of KYC entails identifying the customer and verifying the identity by using reliable and independent documents or information. Not only does a reference account provide an additional proof of identity but also proof of address.

It is important to note that the European adoption of the reference bank account requirement is still subject to approval by BaFin.

5.2 Full KYC

As previously detailed in *D 8.1 Report on European Focus Countries*, the Federal Financial Supervisory Authority (BaFIN) is under the Banking Act (Gesetz über das Kreditwesen - KWG) mandated to monitor the guidelines which are considered when legitimizing a user during account opening.

In order to establish the identity of a VIMpay account holder, the following information has to be collected; name, place of birth, date of birth, nationality and address as instructed under the Money Laundering Act (Geldwäschegesetz – GwG) Part 2 (Due diligence requirements and internal controls and safeguards) section § 4 paragraph 3, part 1 (Identification)

With PayCenter as the selected VIMpay account issuer, the collection of the following VIMpay user details satisfies all BaFin requirements:

a) Name
b) Street Address
c) Document number
d) Date of birth
e) Place of birth
f) State affiliation
g) Issuing authority
h) Nationality

Implementation of the Full KYC will be accomplished through the following 2 options:

5.2.1 PostIdent

The VIMpay physical identity check will be implemented through PostIdent. The physical inspection of the identification documents will have to be conducted by a trusted third party who will ensure that the legitimization requirements as mandated by BaFin are fully met. The current trusted third party in Germany is Deutsche Post.

5.2.2 VideoIdent

The VIMpay online identity check will be implemented through VideoIdent. The identification process conducted through a third party (facilitated by Arvato Betelsmann) will satisfy legitimization requirements which are essential for the Full KYC check of VIMpay EU users. The data collected will be in line with the legitimization requirements set out by BaFin.

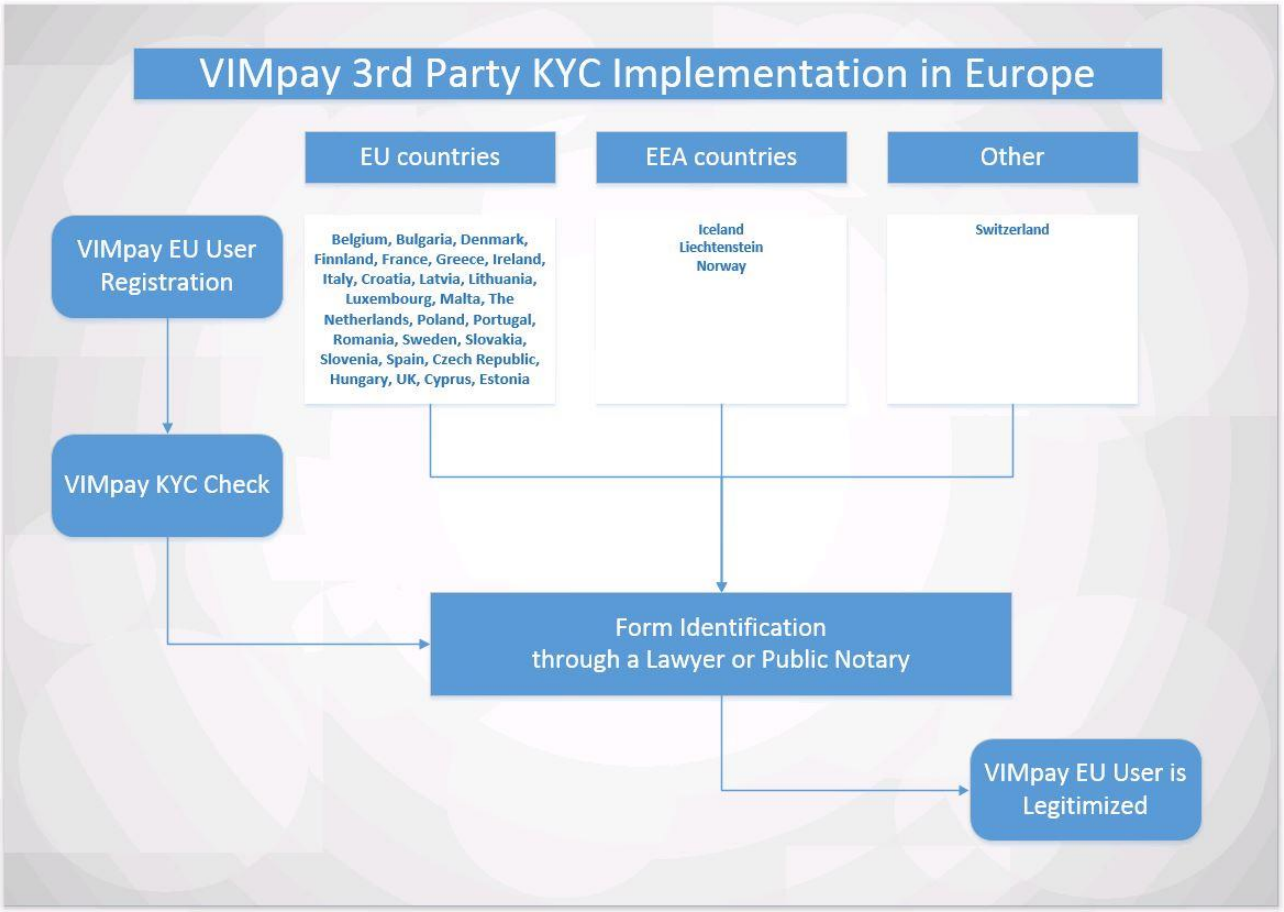
5.3 Third Party KYC

The VIMpay Third Party KYC model will involve the certification of customer identification documents by lawyers or notary after a VIMpay account registration originating from European countries. Identification documents must be certified by suitable third parties in the EU countries and confirmation from the user's previous bank obtained where possible. Suitable third parties include advocates, public notaries, commissioners of oath, judges, magistrates and certain government officials. This VIMpay Third Party KYC model requires a lawyer or notary to apply identity verification rules and use reasonable efforts to ascertain a user's identity.

5.3.1 Implementation

As illustrated below, the process involves presenting a two-sided form and identification documents to a lawyer or registered notary with a request to confirm the information as shown on the customer's identity card or passport.

Once satisfied with the identity of the VIMpay customer and the authenticity of the documentation, the lawyer or notary then affixes their stamp or seal on the document and indicates the office address.



5.3.2 Competitive Advantage

The Third Party KYC model offers VIMpay a very huge competitive advantage. By allowing the verification and certification of identity documentation as an alternative, VIMpay will offer a very competitive upgrade process.

5.4 VideoIdent uncertainty

There has recently been uncertainty surrounding the implementation of VideoIdent by E-Money institutions. To guarantee project cintinuity, petaFuel has opted to pursue other alternatives which are in line with the VIMpay strategy and vision.

5.4.1 Current Federal Financial Supervisory Authority (BaFin) Position

BaFin has opted to treat E-Money institutions (domestic and foreign) differently from banks. Only credit institutions or banks within the meaning of § 1 paragraph 1 of the Banking Act of Germany can utilize VideoIdent. Payment institutions and E-Money institutions may no longer use VideoIdent to legitimize customers. This position has not fully been clarified and BaFin is under advisement to make the clarification.

Furthermore, VideoIdent can only be used by customers who already have an account to make a reference transfer. This effectively stops the usage of VideoIdent for unbanked customers.

5.4.2 Risk Mitigation

The current BaFin position might present some vulnerabilities or risks. However, these project risks can be reduced and mitigated by several countermeasures:

a) 3rd Party KYC Process to address unbanked customers

As illustrated above, the VIMpay 3rd Party KYC process presents VIMpay with a very competitive advantage. The inclusion of a two-sided form and identification documents, which are then verified by a lawyer or registered notary, ensures that the VIMpay audience keeps growing.

This process mitigates any potential project risks by allowing continued VIMpay user acquisition in the EU while still conforming to BaFin regulations.

Currently VIMpay is the only application that allows this type of user legitimization.

b) Small KYC for Europe to support BaFin requirements for reference account

The VIMpay Small KYC model will also be employed in Europe in alignment with BaFin regulations. As required by BaFin, a reference bank account will be required in order to complete the Basic and Plus versions of VIMpay. An additional mobile phone number verification via TAN and an automatic address check will be conducted.

This mitigates VIMpay project risks that might arise from the new regulations.

c) Authorization Process and Negotiations

Considering that PayCenter as the first to be licensed E-Money institute with its own bank code can be considered as more than an E-Money institution, they have initiated private consultations with BaFin in a bid to obtain to obtain the authorization to continue the use of VideoIdent. The consultations are on-going.

6 EU Market Research

The overview below provides information on fundamental regulatory requirements that we have to be aware of as part of the VIMpay expansion into Europe. This includes fundamental KYC requirements, regulators' views on the use of the risk based approach, dealing with Politically Exposed Persons ("PEPs") and other prohibitions that might impact VIMpay. Also included are an insight into the AML requirements and questions on reporting obligations, AML audits and data privacy that are relevant to VIMpay.

6.1.1 Fundamental regulatory requirements for EU countries

AUSTRIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	There are six different circulars in place regarding AML / CFT regulations for the banking industry, other financial services and insurance companies, issued by the Austrian Financial Markets Authority (https://www.fma.gv.at/en/legal-framework/circulars/money-laundering-terrorism-financing.html). [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, one-off transactions below EUR15,000 if there is no AML or CFT suspicion. [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Identification and verification is performed using official ID e.g. passport. Customers have to inform the institution if they act on their own account, or on a principal's account. If someone acts on behalf of another person (as a trustee), the identity of that person (the trustor) must also be clarified. The customer has to disclose the ultimate beneficial owner. The institution has to recheck the identity of the ultimate beneficial owner using a risk based approach. Individuals: The following has to be obtained: a) full name; b) date and place of birth; c) nationality; d) address; and e) signature. As part of the verification process, the identity of the customer has to be verified by an independent source (documents of identification), e.g. a passport, identity card or an Austrian driving licence. The name of the state authority which issued the document and the date of issuance also have to be recorded. Legal entities: the following has to be obtained: a) registered name and domicile of the entity; and b) full name of the legal representatives of the entity. This data has to be verified by 'appropriate documentation' e.g. an excerpt of the company register. [1] [2]

	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	The requirements are defined and are to be seen as a way to rely on the authenticity of the document; if there are any doubts then the identity of a person should be verified by other measures. In this case, a suspicious activity report has to be considered. [3] [1] [4]
	In what circumstances are reduced/simplified due diligence arrangements available?	Reduced due diligence arrangements are available for the following, but only if the AML/CFT risk is considered low: a) domestic public authorities and public authorities of the European Union ("EU"); b) listed companies; c) credit and financial institutions situated in a third country which impose requirements equivalent to those defined in the third EU AML Directive and which are supervised in compliance with those requirements; and d) beneficial owners of pooled accounts held by notaries and other legal professionals from EU Member States. [1] [5]
	In what circumstances are enhanced customer due diligence measures required?	For customers where a higher risk of money laundering or terrorist financing applies, for example: a) if the customer has not been physically present for identification (distance business/non-face-to-face-relationships); b) for cross-frontier correspondent banking relationships with correspondent banks from other countries or from the European Economic Area ('EEA') (the latter only if the AML/CFT risk is considered heightened); and c) for Politically Exposed Persons ("PEPs") of other EU Member States and of third countries [4] [1] [5]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	In any transaction or business relationship with a PEP of another EU Member State (except Austria) or another country. [1] [5]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Enhanced due diligence procedures to be performed for cross-border correspondent banking relationships with correspondent banks from third countries or from the EEA (the latter only if the AML/CFT risk is considered heightened) as follows: a) credit institutions and financial institutions must gather sufficient information about a correspondent bank to fully understand the nature of its business and be able to ascertain the reputation of the institution and the quality of supervision on the basis of publicly available information; b) credit institutions and financial institutions must satisfy themselves of the correspondent bank's anti-money laundering and anti-terrorist financing controls; c) credit institutions and financial institutions must obtain approval from senior management before establishing new correspondent banking relationships; d) credit institutions and financial institutions must document the respective responsibilities of each institution; and with respect to payable-through accounts, credit institutions and financial institutions must be satisfied that the correspondent bank has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent, and that it is able to provide relevant customer due diligence data to the correspondent bank upon request. [2] [1]

	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Non face-to-face relationships and transactions are considered heightened AML/CFT risk by the relevant Austrian AML laws and regulations. For this reason, additional due diligence is always required for non face-to-face relationships and transactions. Trustees must always be identified personally (obligation of personal presence) - non face-to-face relationships are not sufficient for purposes of identification of trustees. Furthermore, additional due diligence is always required (whether face-to-face or non-face-to-face) in the case of any doubts, indication or suspicion of money laundering or terrorist financing. In these cases, suspicious activity reports have to be considered. [3] [5] [1]
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Suspicious activities regarding money laundering and terrorist financing as well as the suspicion that a client might not properly have disclosed a trusteeship have to be reported. [2] [1]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Yes. [1] [5]
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Austria has established a data protection act. It has been in force since 1 Jan 2000 (https://www.dsb.gv.at/DocView.axd?CobId=41936): a) see the definition in Section 4 Data Protection Act: "Data" ("Personal Data") [Daten" ("personenbezogene Daten")]: Information relating to data subjects (sub-para. 3) who are identified or identifiable; Data are "only indirectly personal" for a controller (sub-para. 4), a processor (subpara.5) or recipient of a transmission (sub-para. 12) when the Data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means; "Data Subject" ["Betroffener"]: any natural or legal person or group of natural persons not identical with the controller, whose data are processed (sub-para. 8); b) see above (data subject); and c) see the definition in Section 4 Data Protection Act: "Sensitive Data" ("Data deserving special protection") ["sensible Daten" ("besonders schutzwürdige Daten")]: Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life; The use of sensitive data does not infringe interests in secrecy deserving only and exclusively in the special cases as set out in § 9 data protection act. [5] [1] [6]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Austrian Banking Act. [1]

BELGIUM		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	There is specific guidance per sector on the website of the Belgian Financial Intelligence Processing Unit ('CTIF-CFI') for a risk-based approach: http://www.ctif-cfi.be/website/index.php?option=com_content&view=article&id=71&Itemid=99&lang=en [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, when the customer wishes to carry out a transaction outside the context of a business relationship: a) for an amount below EUR10,000 (art. 7, §1, 2°, a); and b) consisting in a transfer of funds to a payee's account within Belgium for an amount less than or equal to EUR1,000 on condition that (art. 7, §1, 2°, b) these transfers are not considered to fall under the Regulation on information on the payer accompanying transfers of funds (No. 1781/2006): 1. the transfer is a payment within the terms of an agreement for the provision of goods or services, concluded between the payer and the payee; 2. the payee's account was opened to enable the payment for the provision of goods or services; 3. the payment service provider of the payee is subject to the obligations set out in the Law of 11 Jan 1993; and 4. this payment service provider is able, by means of a unique identifier, to trace the transaction via the payee back to the payer. If customers wish to carry out a financial transaction related to gaming for an amount less than or equal to EUR1,000) (art.9). Companies are not obliged to carry out the identification and identity verification of the following persons (art. 11, §1): a) a credit or financial institution, as referred to in Article 2 of Directive 2005/60/EC, situated in Belgium or in another country of the European Economic Area; b) a listed company whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in a country of the European Economic Area; c) the beneficial owners of pooled accounts held by notaries and other independent legal professionals established in Belgium, in another country of the European Economic Area; d) a customer or beneficial owner that is a Belgian public authority; and e) customers that are European public authorities or institutions. Companies are not obliged to carry out the identification and identity verification of the following products or transactions (art. 11, §2): a) life insurance policies where the annual premium is no more than EUR1,000 or the single premium is no more than EUR2,500; b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; and c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest.

		The above exceptions cannot apply where there is a suspicion of money laundering or terrorist financing or when there are doubts about the veracity or accuracy of previously obtained identification data regarding a customer who has already been identified. [5] [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals and institutions must identify clients and their agents. Identification of natural persons: surname, first name, date and place of birth and, whenever possible, relevant information on the address of the identified person (art. 7, §1, paragraph 3). Identification for legal persons, trusts, fiduciaries and similar legal arrangements: corporate name, registered office and directors, and note must be taken of the provisions regarding the power to commit the legal person, trust, fiduciary or similar legal arrangement (art. 7, §1, paragraph 4). The identification must be verified by means of a supporting document, of which a copy is made on paper or by electronic means. For natural persons, a copy of their identity card or passport is required and for legal person, a copy of their coordinated statutes (art. 7, §2). Together with the identification, information must be collected regarding the purpose and intended nature of the business relationship (art. 7, §1, paragraph 5). [5] [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Clients must be identified by means of a supporting document, of which a copy is made on paper or by electronic means (art. 7, §2). Such documents need to be probative documents, admissible as evidence. There is no information about certification by external third parties in local legislation. [5] [1] [4]
	In what circumstances are reduced/simplified due diligence arrangements available?	The local regulation does foresee this possibility where (art. 11, §1): a) the customer or beneficial owner is a credit or financial institution as defined in art. 2 of the third AML Directive, established in Belgium or another country within the EEA, or an equivalent institution established in a third country that has foreseen requirements and controls similar to those in the third AML Directive and of which a specific list is to be drawn in a Royal Decree; b) the customer or beneficial owner is a listed company whose securities are admitted to trading on the regulated market within the meaning of Directive 2004/39/EC in a country of the EEA, or is a listed company from a third country, designated in a Royal Decree, and which is subject to disclosure requirements consistent with community legislation; c) the beneficial owner of a pooled account held by notaries and other independent legal professionals established in Belgium or another country within the EEA or from third countries, designated in a Royal Decree, provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts. If the client would be bound by professional secrecy, and thus unable to provide the information on the identity of the beneficial owner, the client needs to confirm in writing or by electronic means to the depository institution that the beneficial owners of the pooled accounts involved are solely clients with whom the relationship consists in ascertaining their legal position or performing their task of defending or representing those clients in, or concerning judicial proceedings including giving advice on instituting or avoiding proceedings. The client or beneficial owner is a Belgian public authority; d) the client is a European public authority or institution, included on a list to be drawn in a Royal Decree; and e) the client is a person or institution indicated in a specific list yet to be drawn in a Royal Decree.

		In addition, by way of derogation, it is allowed not to apply customer or beneficial owner due diligence in respect of (art. 11, §2): a) life insurance policies where the annual premium is no more than EUR1,000 or the single premium is no more than EUR2,500; b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; d) electronic money as defined in article 3, §1, 7° of the law of 22 Mar 1993 regarding the pursuit of and prudential supervision of credit institutions, where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR150, or where, if the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR1,000 or more is redeemed in the same calendar year by the bearer as referred to in article 5 of the law of 22 Mar 1993; and e) in respect of any other product or transaction representing a low risk of money laundering or terrorist financing which meets the criteria to be established in a royal decree. If customers wish to carry out a financial transaction related to gaming for an amount less than or equal to EUR1,000 (art. 9). [5] [1] [4]
	In what circumstances are enhanced customer due diligence measures required?	Local regulation foresees enhanced customer due diligence measures on a risk sensitive basis in situations which by their nature can represent a higher risk of money laundering or terrorist financing, and at least in the following situations (art. 12, §1): a) establishing a business relationship with or carrying out a transaction for a customer that was not physically present for identification purposes (non face-to-face contact) (art. 12, §2); b) establishing a business relationship or carrying out a transaction with or for a PEP (art. 12, §3) (see A14 below); and c) engaging in cross-border correspondent banking relationships with respondent institutions from third countries (art. 12, §4) (see A15 below). [1]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Belgium has instituted a comprehensive set of measures applicable to PEPs. These measures include (art. 12, §3, paragraph 4): a) applying appropriate risk based procedures to determine whether the customer or his beneficial owner is a PEP; b) obtaining approval from a sufficiently senior level of management before establishing business relations with such customers; c) taking appropriate risk-based measures to establish the source of wealth and funds that are involved in the business relationship or transaction; and d) conducting enhanced ongoing monitoring of the business relationship. [1]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Belgium is in full compliance with the FATF recommendations regarding issues of correspondent banking. It is obliged to (art. 12, §4, paragraph 1): a) gather sufficient information about the respondent institution in question to understand fully the nature of its business and to determine from publicly available information its reputation and the quality of the supervision to which it is subject;

		b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls; c) obtain approval from a sufficiently senior level of management before establishing new relationships; d) document in writing the respective responsibilities of each institution; and e) with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of and has performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request. [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	When entering into a business relationship with a client that is not physically present, specific and adequate measures need to be taken to deal with the increased risk of money laundering and terrorism financing that exist in such circumstances (art. 12, §2).
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	The institutions and persons as referred to in the law, shall carefully examine any transaction or action they consider particularly likely, by its nature or its unusual character in view of the customer's activities, by the circumstantial elements or by the capacity of the persons involved, to be related to money laundering or terrorist financing (art. 14, §1, paragraph 2). The following institutions and persons should report the following transactions: a) the sales price of real property may only be paid by means of a bank transfer or cheque. The agreement and deed of sale must specify the number of the financial account from which the amount was or will be debited (art. 20); b) in case of doubt about the veracity or accuracy of previously obtained identification data about a customer who has already been identified (discretionary) (art. 7, §1, 4°); c) in case of a suspicion of money-laundering or terrorism financing (art. 23 – 26); d) in case of international transactions and facts involving natural or legal persons domiciled, registered or situated in a country or territory whose legislation is considered insufficient by a competent international consultative and coordinating authority or whose practices are deemed by this authority to impede the fight against money laundering and terrorist financing (art. 27); e) in case of the suspicion of serious and organised fiscal fraud (art. 28).
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No. [5] [1]
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data?	Yes, if you are processing personal data in Belgium, you are subject to the Belgian Privacy Act of 08 Aug 1992: a) yes. Personal data is defined as any information relating to an identified or identifiable natural person, hereinafter the 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Article 1 §1 Privacy Act.). Personal data covers any information relating to an identified or identifiable natural person, e.g. name, address bank account, education, images, GPS data, IP address, etc.;

	c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	b) as mentioned, the scope of protection of this Act only covers natural persons (private individuals) not legal persons. Corporate data is therefore not protected under privacy law in Belgium, unless it relates to private individuals (e.g. HR data); c) yes. By principle, the processing of sensitive data is forbidden (exceptions exist). Sensitive data relate to race, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, prosecutions or criminal or administrative convictions (art. 6 Privacy Act). [5] [6]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	There exists specific privacy legislation for certain sectors e.g. public sector, telecom sector which apply in addition to the Privacy Act mentioned above.

BULGARIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Bulgaria is a member of the Financial Action Task Force (FATF), as well as the Committee of Experts on the Evaluation of Anti-Money Laundering Measures & the Financing of Terrorism (MONEYVAL) and the Egmont Group. [7] [8] [2]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, transactions below 15.000 Euros if there is no AML or CFT suspicion. [7] [8] [9]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: should provide a valid document with: Full name, signature, date of birth, nationality, address, profession, work address, tax identification number and photo and politically exposed job/function, purpose. Legal persons: should provide a valid document with the headquarters address, identification number, shareholder identification for individuals who hold more than 25% of the voting rights and identification of the board of directors. For non-resident entities, equivalent documentation is required. [7] [8] [9]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Passports or other valid personal identification documents must be certified by a Notary. [2]
	In what circumstances are reduced/simplified due diligence arrangements available?	No allowance for simplified procedures is provided [9] [4]
	In what circumstances are enhanced customer due diligence measures required?	The law requires banks to adopt procedures for mitigating risks arising from PEPs [9] [4]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	There are enhanced due diligence procedures for domestic PEP.

	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Prior to the creation of a correspondent banking relationship, the following is required: a) sufficient information on the relevant correspondent institution and the nature of its operations; b) publicly sourced information to establish the quality of supervision overseeing the correspondent institution; c) an evaluation of measures applied by the correspondent institution against the legitimisation of proceeds of crime and financing terrorism; d) understanding if approval of relevant lead employee to open the corresponding bank relationship was granted; and e) in the case of wire transfers, confirmation from the correspondent bank that it has identified the account holder. [8] [7] [9]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Where a customer approaches a firm remotely (by post, telephone or over the internet), the firm should carry out non face-to-face verification, either electronically, or by reference to identification documents [7] [8] [9]
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Mandatory reporting of all cash transactions in excess of 15.000 Euros [7] [9]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Bulgaria has data protection laws in place. a) No - SG No. 70/10.08.2004, amended, SG No. 103/2005 b) the data protection law does not apply to corporate data as the definition of data subject does not include a company. Corporate data may be protected contractually by confidentiality agreements; c) No. [7] [8] [9]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	No.

CROATIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes, there are several guidelines available: The Croatian National Bank's Guidelines for the implementation of the Anti - Money Laundering and Terrorist Financing Act with respect to credit institutions, credit unions and electronic money institutions: http://www.hnb.hr/novcan/pranje_novca_terorizam/e-smjernice-zakon-spnft-ki-en.pdf The Croatian Financial Services Supervisory Agency Guidelines for the implementation of the Anti- Money Laundering and Terrorism Financing Act for obligated persons who fall within the supervisory scope of the Croatian Financial Services Supervisory Agency (Croatian version only): http://www.hanfa.hr/ Ministry of Finance – Financial Inspectorate: a) general guidelines for the implementation of the Anti -Money Laundering and Terrorism Financing Act (http://www.mfin.hr/en/anti-money-laundering-office); b) guidelines for the implementation of the Anti-Money Laundering and Terrorism Financing Act for audit firms, independent auditors, natural and legal persons who provide accounting and tax counselling services (Croatian version only) (http://www.mfin.hr/adminmax/docs/Sektorske_smjernice_za_revizore_itd.pdf); c) guidelines for the implementation of the Anti-Money Laundering and Terrorism Financing Act for lawyers and public notaries (Croatian version only) (http://www.mfin.hr/adminmax/docs/Smjernice_ZSPNFT_odvjetnici_i_javni_biljeznici.pdf); d) guidelines of the Office for Money Laundering Prevention of the Ministry of Finance (Croatian version only) (http://www.mfin.hr/hr/zakoni-i-pravilnici); and e) latest general guidelines from Jul 2015: (http://www.mfin.hr/adminmax/docs/Opce%20smjernice%20FI_rev2015.pdf). [5] [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, one-off transactions below HRK105,000 (approx. USD14,830) in total, whether carried out as a single operation or several linked transactions reaching the prescribed threshold. In addition, electronic money institutions from another Member State and branches of third-country electronic money institutions may be exempt from the obligation to carry out customer due diligence measures in the following cases: a) when issuing electronic money, if a single amount of a payment executed for the issuance of such money, on an electronic data carrier which may not be recharged, does not exceed the HRK equivalent of EUR150 (approx. USD160); and b) when issuing electronic money and dealing with electronic money, if the total amount of executed payments, stored on an electronic data carrier which may be recharged, does not exceed the HRK equivalent of EUR2,500 (approx. USD2,710) during a calendar year, except in the cases where the electronic money holder cashes the HRK equivalent of EUR1,000 (approx. USD1,090) or more during the same calendar year. Credit institutions may be exempt from the obligation to carry out the customer due diligence measures in the case of other products or transactions associated with them, which pose negligible ML/TF risks,

		provided they meet the conditions prescribed by an ordinance of the Minister of Finance. Insurance companies licensed for the performance of life insurance business, insurance companies from member-states with a business unit in Croatia or authorised to directly perform life insurance business in Croatia, pension companies, as well as legal entitles and individuals performing business or activity of insurance representation or intermediation for entering into life insurance agreements may be allowed not to carry out customer due diligence in the following cases: a) contracting life insurance policies in which the individual premium instalment or several insurance premium instalments to be paid within one year does not exceed a total HRK equivalent amount of EUR1,000 (approx. USD1,090), or in cases when single premium payment does not exceed the HRK equivalent value of EUR2,500; and b) contracting pension insurances providing that types of insurance are being contracted whereby it is not possible to transfer the insurance policy to a third person or use it as collateral for a credit or loan, and a contract is entered into with a closed-end pension fund if the employer pays the contributions into the voluntary pension fund on behalf of the fund's members (no monetary threshold indicated). Institutions and persons may not be exempt from the obligation to carry out customer due diligence measures when there are grounds for suspicion of ML/TF with respect to a customer, product or transaction. [5] [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Identification and verification of an individual's identity is done through examination of the original customer's personal identification documents in the customer's presence (e.g. an ID Card for residents and a passport for non-residents). Individuals: a) full name and surname; b) permanent address; c) date of birth; d) place of birth; e) personal identification number; and f) name and number of the identification document, the name of the issuing authority. Legal entities: Verification of legal entities' information is done through examining documentation from court or other public register. The following data should be collected and verified: a) registered name; b) registered seat (street and number, place and country); c) business registration number; d) full name and surname, permanent address, date of birth place of birth, personal identification number, name and number of the identification document, the name of the issuing authority of a legal representative/person acting on behalf of a legal entity on the basis of Power of Attorney; and e) name and surname, permanent address, date of birth and place of birth of the beneficial owner. If there is any suspicion during the course of identifying the legal person and verifying the legal person's identity as to the veracity of data collected or credibility of the documents and other business documentation from which data was collected, the institution or person performing identification and verification shall ask the legal representative or the person authorised by

		power of attorney to give a written statement prior to establishing a business relationship or executing a transaction. [5] [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Identification and verification of an individual's identity is done through examination of the original customer's personal identification documents in the customer's presence. In case of legal entities, identification and verification is performed by examining an original or a notarised copy of documentation from court or other public register presented by the legal person's legal representative or person authorised by power of attorney. At the time of submission, the originals or the notarised copies of the required documentation must not be more than three months old. The legal entity's identity can be also identified and verified by gathering the required data through a direct examination of court or other public register. The copy of the excerpt from the register examined directly must be endorsed i.e., the examiner must put date, time, his/her name and surname. While verifying customer's identity, the institutions and persons performing identification and verification must first check the nature of a register from which data for the identity verification purposes are obtained. Identification and verification of the legal representatives of legal entities, persons who act on behalf of a legal entity on the basis of the Power of Attorney and representatives of the trust, foundations or NGOs is done thorough the examination of original personal identification documents of those persons in their presence. If the documents are insufficient to collect all prescribed data, the missing data are collected from other valid public document submitted by those persons i.e. from those persons directly. Beneficial owner's identification and verification is done by examining the originals or notarised copies of documents from a court or other public register not more than three months old at the time of their submission. If those documents are insufficient for collecting data on beneficial ownership, then examination of the original or notarised documents and other business documentation supplied by the legal representative or person authorised by power of attorney is performed or data is collected directly from a written statement given by the customer's legal representative or the person authorised by power of attorney. [5] [1]
	In what circumstances are reduced/simplified due diligence arrangements available?	Reduced/simplified due diligence arrangements are possible in respect of customers or products or transactions representing a low risk money laundering or terrorist financing risk except in instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a customer or a transaction. This applies to relationships or transactions with the following: a) credit or financial institutions from the EU/EEA states or third countries considered as having equivalent AML/CFT systems to the EU (banks, savings bank, housing savings banks, Croatian Post, investment funds management companies, pension funds companies, financial instruments companies' insurance companies who provide life insurance services); b) companies listed on a regulated market in the EU states or from the third countries which are subject to disclosure requirements consistent with the EU legislation; c) domestic public authorities and the public authorities of the EU; and d) persons who meet the conditions set forth by the Ordinance on the determination of conditions under which institutions and persons identify customers who pose a negligible risk in terms of money laundering or terrorist financing. [5] [1] [4]
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence measures and enhanced ongoing monitoring is required in any situation which due to the nature of the business relationship, the form and manner of transaction execution, business profile of the customer or other circumstances associated with the

		customer can present a greater risk of money laundering or terrorist financing. Three specific types of relationships where enhanced due diligence measures must be applied are: a) where the customer has not been physically present for identification and identity verification purposes; b) in respect of a correspondent banking relationship with respondents from non-EU/EEA states; or c) in respect of a business relationship with a PEP. [5] [1] [4]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	In any transaction or business relationship with a PEP from a country other than Croatia ('a foreign PEP'). [5] [1] [4]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Enhanced due diligence measures must be applied in respect to correspondent relationship with a bank or other credit institution from a third country (non-Member States of the EU/EEA) and the following additional data and documentation must be gathered in the process: a) the date of issuance and validity period of authorisation to provide banking services, and the name and seat of a competent third-country authority that issued the authorisation; b) a description of the implementation of internal procedures relating to ML/TF prevention and detection, particularly the procedures of customer identity verification, beneficial owner identification, reporting to the competent bodies on suspicious transactions and customers, record keeping, internal audit and other procedures that the bank or other credit institution adopted in relation to ML/TF prevention and detection; c) a description of systemic arrangements in the field of the ML/TF prevention and detection in effect in a third country in which the bank or other credit institution has its seat or in which it has been registered; d) a written statement confirming that the bank or other credit institution does not operate as a shell bank; e) a written statement confirming that the bank or other credit institution neither has business relationships with shell banks established, nor does it establish business relationships or conduct transactions with shell banks; and f) a written statement confirming that the bank or other credit institution falls under the scope of legal supervision in the country of its seat or registration, and that it is required to apply legal and other regulations in the field of the ML/TF prevention and detection in accordance with that country's effective laws. In order to establish new correspondent banking relationships, a prior written approval of a credit institution's senior management must be sought. In the context of enhanced due diligence, credit institutions must obtain the following additional documentation: a) a written statement that the correspondent bank or other credit institution has verified the identity of a customer and that it conducts ongoing due

		diligence of customers who have direct access to payable-through accounts, and b) a written statement that the correspondent bank or other credit institution can provide, upon request, relevant data obtained on the basis of due diligence of customers having direct access to payable-through accounts. [5] [1] [4]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Non-face-to-face transactions and/or relationships are considered higher risk of ML/TF by the Croatian AML/TF Act and other relevant regulations. Where a customer has not been physically present for identification purposes, enhanced customer due diligence must always be performed. In such cases, institutions and persons covered by the Croatian AML/FT Act must apply one or more of the following supplementary enhanced due diligence measures: a) obtain additional documents, data or information on the basis of which the customer's identity shall be verified; b) additionally verify the submitted documents or additionally certify them by a foreign credit or financial institution; and/or c) apply a measure whereby the first payment within the business activity is carried out through an account opened in the customer's name with the given credit institution. Establishing a business relationship without physical presence of the customer is not permitted, unless a reporting entity applied those additional measures. Pursuant to the Croatian AML/FT Act credit and financial institutions are obliged to pay special attention to any ML and/or TF risk which may stem from new technologies enabling anonymity (Internet banking, ATM use, tele-banking, etc.) and put policies in place and take measures aimed at preventing the use of new technologies for the ML/or TF purposes. They must have policies and procedures in place for risks attached with a business relationship or transactions with non-face-to-face customers and to apply them at the establishment of a business relationship with a customer and during the course of conducting customer due diligence measures which include the supplementary measures described above. [5] [1] [4]
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Yes, besides an obligation to report suspicious transactions, there is an obligation to report to the Anti-Money Laundering Office on each transaction being conducted in cash totalling HRK200,000 (approx. EUR28,000 or USD30,430) and more immediately, and no later than within three days upon the execution of the transaction. The Act also mandates that a special attention is paid to all complex and unusually large transactions, as well as to each unusual transaction without an apparent economic or visible lawful purpose even when the reasons for suspicion of the ML/TF have not been detected. However, if the reasons for suspicion are detected in relation to such transactions, they should be reported to the Office. In all instances when the customer seeks an advice from persons involved in the performance of professional activities on money laundering or terrorist financing, the persons involved in the performance of professional activities must immediately notify the Office thereof, and no later than within three business days from the date the customer sought for such an advice. [5] [1] [4]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and	No. Only a regular internal AML audit is required by the law. [1]

	controls?	
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Croatia has data protection laws in place. a) yes; b) no clear rules regarding corporate data; and c) yes; sensitive data is defined as information covering the racial or ethnic origin of the data subject, political opinions, religious or other beliefs of a similar nature membership of trade unions, physical or mental health or condition, sexual life and personal data regarding criminal and misdemeanour proceedings. In principle, such data cannot be processed, and derogation is tolerated under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, carrying out legal obligations to which personal data filing system controller is subject, or if the data subject discloses such data on his/her own. Such data has to be specifically labelled and protected. Therefore, any information assets (information systems, computers) that store or process sensitive data are also assigned a high level of protection. The additional protections of sensitive data are set forth in the Regulation on the manner of storing and special measures of technical protection of the special categories of personal data (Official Gazette, No. 139/04). [5] [1] [4]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	EU case law on data protection (European Court of Justice cases) has applied to Croatia since 01 Jul 2013 (accession date) and may impact on the transfer of information.

CYPRUS		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	The Institute of Certified Public Accountants of Cyprus ("ICPAC") has issued a Directive for the Prevention & Suppression of Money Laundering & Terrorist Financing Laws of 2007 and 2010 that serves asguidance to audit firms. The latest version was issued in Sep 2013. [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, occasional transactions under EUR15,000 whether the transaction is carried out in a single operation or in several operations which appear to be linked. [5] [1] [4]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Due diligence measures comprise identifying and verifying the identity of the beneficial owner owning or controlling more than 10% of the shares or voting rights of the client.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	The documents must be certified true copies of the originals.
	In what circumstances are reduced/simplified due	According to paragraph 63-(1) of the Law:

	diligence arrangements available?	Simplified customer due diligence and identifications procedures can be used in respect of the following: a) credit of financial institution covered by the EU Directive or those who are situated in a country outside the European Economic Area which: a. in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, imposes requirements equivalent to those laid down by the EU Directive; and b. it is under supervision for compliance with those requirements; b) listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or in a third country which is subject to disclosure requirements consistent with community legislation; and c) Domestic Public Authorities of countries of the European Economic Area. [5] [1] [4]
	In what circumstances are enhanced customer due diligence measures required?	According to paragraph 64-(1) of the Law: Enhanced due diligence measures should be in place in respect of the following customers: a) where the customer has not been physically present for identification purposes; b) in respect of cross-frontier correspondent banking relationships with current institutions to customers from third countries; and c) in respect of transactions or business relationships with politically exposed persons ('PEPs') residing in a country within the European Economic Area or a third country. According to paragraph 64-(2) of the Law: "Enhanced customer due diligence measures must be taken in all other instances which due to their nature entail a higher risk of money laundering or terrorist financing." [5] [1] [4]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	According to paragraph 5.61 of the Directive, if the prospective client is a PEP, the firm should obtain senior management approval for establishing business relationship. In addition, according to paragraph 4.55 of the Directive, the firm should establish the source of wealth and source of funds for PEPs and also conduct ongoing monitoring on the business relationship. Paragraph 5.62 of the Directive states that the firm should pay special attention when PEPs originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent to international standards. With regards to the issue of corruption, a useful source of information is the Transparency International Corruption Perceptions Index which ranks countries and territories based on how corrupt their public sector is perceived to be. [5] [1] [4]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	According to 64 (b) of the Law, in respect of cross-frontier correspondent banking relationships with credit institutions to customers from third countries, it is required to: a) gather sufficient information about the credit institution customer to fully understand the nature of the business and the activities of the customer and to assess, from publicly available information, the reputation of the institution and the quality of its supervision;

		b) assess the systems and procedures applied by the credit institution customer for the prevention of money laundering and terrorist financing; c) obtain approval from senior management before entering into correspondent bank account relationships; d) document the respective responsibilities of the person engaged in financial or other business activities and of the credit institution customer; and e) with respect to payable-through accounts, it must be ensured that the credit institution-customer has verified the identity of its customers, and performed ongoing due diligence on the customers having direct access to the correspondent bank accounts and that it is able to provide relevant customers' due diligence data to the correspondent institution, upon request. [5] [1] [4]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	If the client is a non-Cypriot resident who is not seen face-to-face, then a professional adviser in the client's home country could be used to confirm identity, or a copy of the passport authenticated by an attorney or consulate, or verification details covering true name, permanent address and verification of signature could be checked with a reputable credit or financial institution or professional advisor in the prospective client's home country.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	According to 6.05 of the Directive, any knowledge or suspicion of money laundering or terrorist financing should be promptly reported to MOKAS [1]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	In accordance with the Central Bank of Cyprus "Directive on a Framework of Principles of Operation and Criteria of Assessment of Banks' Organisational Structure, Internal Governance and Internal Control Systems of 2006 to 2012" ("the CBC Directive") banks should submit to the Central Bank of Cyprus a report prepared by external auditors/consultants every three years, on the assessment of the adequacy of the internal control System on an individual company as well as consolidated group basis. Under the CBC Directive, the external auditor/consultant assesses the internal control environment (including systems) with regard to the banks' management of the risk of money laundering and terrorism financing. [1]
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	a) yes, the Processing of Personal Data (Protection of the Individual) Law of 2001 as amended in 2003; b) the data protection law does not apply to corporate data as the definition of data subject does not include a company. Corporate data may be protected contractually by confidentiality agreements; and c) yes there is a separate definition of "sensitive data". Sensitive data means data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, participation in, association and trade union membership, health, sex life and sexual orientation, as well as on criminal charges or convictions. The collection and processing of sensitive data is prohibited. Any collection or processing of sensitive data requires the consent of the data subject, e.g. in order to go through with a contract with the consent of the data subject e.g. in employment contracts, insurance contracts etc. [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of	Transfer of personal data within the EU is free. For a transfer to a third country, a license must be obtained from the Commissioner of Protection of Personal Data.

	information to this jurisdiction?	
CZECH REPUBLIC		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes, guidelines and methodical recommendations issued by the Ministry of Finance (http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/stanoviska-financniho-analytickeho-utvar). Guidelines also issued by Czech National Bank (http://www.cnb.cz/cs/dohled_financni_trh/legislativni_zakladna/legalizace_vynosu/metodiky_vyklady.html). [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, any single transaction below EUR15,000 does not require any customer due diligence unless it is a: a) a suspicious transaction; b) an agreement to enter into a business relationship; c) an agreement to establish an account, to make a deposit into a deposit passbook or a deposit certificate, or to make any other type of deposit; d) an agreement to use a safety deposit box or an agreement on custody; e) a transaction with a PEP; and f) as part of the business relationship. [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	The following information is required: Individuals: Name, surname, birth identification number or date of birth, place of birth, sex, address and citizenship. These would normally be verified by an identity card or passport. Individuals who conduct business: In addition to the above, full name of the business, place of business and identification number needs to be noted. Legal entities: the full name, residency/seat, identification (or similar identification received from foreign offices) showing evidence of the company's existence (i.e. certificate of incorporation, trade register statement or other). The same principles for individuals apply for the identification of individuals in the company's statutory body. If the company's statutory body or the owner is another legal entity, identification documentation must also be collected for that entity. [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	These should be certified by an appropriate person e.g. a notary, local authorities etc. Specific rules apply to credit and financial institutions, where certain employees are authorised to verify these when opening account, concluding contract etc.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence is applicable for a transaction exceeding EUR1,000 unless it is a: a) suspicious transaction: b) an agreement to enter into a business relationship; c) an agreement to establish an account, to make a deposit into a deposit passbook or a deposit certificate, or to make any other type of deposit; d) an agreement to use a safety deposit box or an agreement on custody;

		e) a life insurance contract, should the customer have a right to pay extra premiums above the agreed limit of the one-off or regular premiums payments; f) a purchase or receipt of cultural heritage, items of cultural value, used goods or goods without a receipt of origin to further trade in such goods, or receipt of such items in pawn; or g) withdrawal of the final balance of a cancelled bearer passbook. [1]
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence is applicable for: a) a remote financial services agreement under the Civil Code; b) a transaction and business relationship with a PEP: and c) a correspondent bank relationship with a foreign credit or similar institution ("Correspondent Institution"). [1]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Legislation requires financial institutions to: a) have sufficient procedures to determine whether the customer is a PEP who is a resident of another country; b) obtain approvals from senior management on a daily basis for establishing business relationships with such customers; c) take reasonable measures to gather information about the sources of income and funds that are involved in the business relationship or transaction; and d) continuously monitor the business relationship. [1]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	All transactions with PEPs are subject to due diligence including the provision of information and supporting documentation relating to: a) the purpose and intended nature of the transactions or business relationship; b) the beneficial owner, if the client is a legal entity; c) the information required for continuous monitoring of the business relationship; and d) a review of the income source. [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	In the case of a remote financial services agreement under the Civil Code, the entity shall review the customer as follows: a) the first payment under this agreement shall be made via an account kept in the customer's name held at a credit institution or a foreign credit institution operating in the European Union ("EU") or the European Economic Area ("EEA"); and b) the customer shall submit to the entity a copy of a document verifying the existence of this account together with copies of the relevant parts of his identity card and at least one more identification document to validate the customer's identification data of this card i.e. the type, serial number, issuing country or institution and validity. [1]
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash	Suspicious transactions are identified based on criteria such as unusual transactions, international wire transfers etc. However, no special report is required.

	transactions above a certain threshold, international wire transfers, other transactions etc.?	
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No. However, if the external auditor during performance of the regular audit procedures finds out facts which indicate suspicion of committing economic crime, crime against property or crime of corruption, he is obliged to inform the FAU, statutory representatives and control body of the given bank thereof. The central bank is however authorised to ask the bank to appoint the auditor for review of their internal control system which might also include a review of the AML function if requested by the central bank.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes. Czech Act No. 101/2000 Coll. on Data Protection ("Data Protection Act") (https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107) governs the area of personal data protection: a) yes; b) corporate data, i.e. data that relate to legal entities, not the natural persons do not fall under the category "personal data" protected under the Data Protection Act; c) yes, the Data Protection Act stipulates a separately protected category of personal data. It is forbidden to process personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or political movements, trade union membership and data concerning health or sex life. [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Transfers of personal data outside EEA and EU have been recently affected by the decision of No. C-362/14 Maximillian Schrems v. Data Protection Commissioner from 06 Oct 2015 of the Court of Justice of the European Union cancelling the Safe Harbor Regime. As a result, the Czech Office for Personal Data Protection recommends to use standard contractual clauses according to the Commission decision No. 2010/87/EU from 05 Feb 2010 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF) and/or Binding Corporate Rules (http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm) to govern the transfer of information to the US. [1]

DENMARK		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	A Danish general guidance is issued by the Danish FSA (http://www.finanstilsynet.dk/da/Temaer/Hvidvask/Regler.aspx). Furthermore, the Danish Business Authority has issued guidance for specific sectors e.g. accountancy sector (https://www.retsinformation.dk/Forms/R0710.aspx?id=146481). [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	As the main principle customer due diligence always applies. However, transactions below EUR6,700 may be exempted from part of the due diligence requirements pursuant to the current regulation and guidelines. A potential exemption from the customer due diligence requirement must be based upon a risk assessment and must comply with all statutory requirements.
	What are the high level requirements for verification	Individuals: name, address and social security number. Accepted evidence includes: passport, driving license, birth certificate, tax returns and tax code

	of customer identification information (individuals and legal entities)?	(including social security number). In addition, electronic public keys (NEM-ID) can function as a supporting document if it is presented together with one or more of the primary documents. Corporates: name, address and company number. Accepted evidence includes: registered information from the Danish Commerce and Companies Agency and Articles of Association. [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	There are no mandatory requirements in the law, but it is stated in local guidance that copies of identification documentation are accepted. Copies of documentation can be certified by financial institutions according to the law.
	In what circumstances are reduced/simplified due diligence arrangements available?	Customer due diligence is reduced in three main areas: a) payments for life insurance or under pension agreements under specific circumstances e.g. payments of EUR1,000 or less for recurring fees and a one-time fee of EUR2,500 or less; b) electronic money - if the device cannot be recharged and the maximum amount stored in the device is no more than EUR250, or where, if the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR1,000 or more is redeemed in that same calendar year; and c) specific transactions and products as described by the Danish Financial Services Agency ("FSA") in order no. 712 of 2008. [1]
	In what circumstances are enhanced customer due diligence measures required?	Local guidance states four cases: a) customers who do not physically present themselves for identification purposes; b) cross-border correspondent banks; c) PEPs; and d) shell companies. [1] [5]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Legislation requires financial institutions to: a) have sufficient procedures to determine whether the customer is a PEP who is a resident of another country; b) obtain approvals from senior management on a daily basis for establishing business relationships with such customers; c) take reasonable measures to gather information about the sources of income and funds that are involved in the business relationship or transaction; and d) continuously monitor the business relationship.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	In cases of money transfers to or from a bank outside the European Union ('EU') where there is no official agreement of financial services with the EU, further proceedings have to be considered as stated in the local guidance. Before establishing new correspondent banking relationships, firms will be required to: a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine, from publicly available information, the reputation of the institution and the quality of supervision;

		b) assess the counterparty's AML and anti-terrorist-financing controls; and c) obtain daily approval from senior management.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	In the case of a customer who has not been physically present for identification purposes, legislation requires the taking of 'further measures to ascertain the customer's identity'. It sets out an illustrative list of measures that can be taken to ascertain the customer's identity in these situations, such as: a) ensuring that the customer's identity is established by additional documentation; b) checking or verifying the documents supplied, or requiring a confirmatory certification by another financial institution; and c) requiring that the first payment in connection with the transactions is carried out through an account opened in the customer's name with a bank.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Any suspicion (that has not been disproved) of a potential violation of the regulation on money laundering and terrorist financing, has to be reported immediately to the relevant authorities.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes: a) yes, the definition of "personal data" will likely cover material held for KYC purposes (please see link below); b) the act on processing of personal data does not apply to corporate data (please see link below); and c) there are no specific definitions of "sensitive data" in the Danish act on processing of personal data. However, sections 6-8 defines three different categories of information: normal personal information (6), sensitive personal information on private matters (7) and other types of information on private matters (8) (please see link below). http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/ [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	This would have to be evaluated by a lawyer.

ESTONIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	The Estonian Financial Intelligence Unit: https://www.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/fius-advisory-guidelines/ The Estonian Financial Supervision Authority: http://www.fi.ee/index.php?id=3375 [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Due diligence measures are always required upon establishment of a business relationship and upon suspicion of money laundering or terrorist financing (regardless of any limits provided by law). Otherwise, there is a EUR15,000 thresholds for transactions (regardless of whether one or several related payments); EUR6,400 upon provision of currency exchange services; EUR2,000 for organisers of games of chance, regarding all persons who pay or receive more than that in a single transaction or several related transactions. [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	An obligated person shall identify a natural person (face-to-face) and verify the person on the basis of an identity document. In addition to an identity document, the representative of a person participating in a transaction shall submit a document in the required format, certifying the right of representation. An obligated person shall identify a legal person and its passive legal capacity and verify the information obtained. Legal persons registered in Estonia and branches of foreign companies registered in Estonia shall be identified on the basis of an extract of a registry card of the relevant register. Foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equivalent document which has been issued by a competent authority or body not earlier than six months before submission thereof.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	A copy shall be made of the page of an identity document submitted for identification which contains the personal data and a photograph. In addition, upon identification and verification the following personal data shall be registered: a) the name and the representative's name; b) the personal identification code or, upon absence of a personal identification code, the date and place of birth; c) the name and number of the document used upon identification and verification of persons, and its date of issue and the name of the agency which issued the document; and d) the name of the document used upon identification and verification of the right of representation, and its date of issue and the name of the issuer. In certain cases, the address of the place of residence and the profession or area of activity of the person shall be registered. A representative of a legal person of a foreign country shall, at the request of an obligated person, submit a document certifying his or her powers, which has been notarised or authenticated pursuant to an equal procedure and legalised or authenticated by a certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence measures can be undertaken if a person participating in a transaction entered into it in economic or professional activities or a person using a professional service or a customer is: a) a legal person governed by public law founded in Estonia;

		b) a governmental authority or another authority performing public functions in Estonia or a contracting state of the EEA; c) an authority of the European Community; d) a company of a contracting state of the EEA or a third country, which is subject to requirements equal to those provided for in Estonian legislation and whose securities are traded in a regulated securities market in one or several contracting state of the EEA; and e) a credit institution or a financial institution, a credit institution or a financial institution located in a contracting state of the EEA or in a third country, which in the country of location is subject to requirements equal to those provided for in Estonian legislation and the performance of which is subject to state supervision. An obligated person may apply the simplified due diligence measures with regard to the beneficial owners of an official account opened by a notary public or enforcement officer of a contracting state of the EEA or third country, provided that the official account is subject to due diligence measures which are in compliance with the international standards for prevention of money laundering and terrorist financing, state supervision is exercised over adherence to these requirements and the notary public or enforcement officer has and preserves information about the identity of the beneficial owner. An insurer or insurance broker may take simplified due diligence measures if: a) a life assurance contract is made whereby the annual assurance premium does not exceed EUR1,000 or a single premium does not exceed EUR2,500; b) a pension insurance contract is made which does not provide for the right of withdrawal or cancellation and which cannot be used as loan collateral; and c) a transaction is entered into in the framework of a superannuated pension scheme or another scheme allowing for such pension benefits whereby insurance premium is debited from wages and the terms and conditions of the pension scheme do not allow for assignment of the rights of a participant in the scheme. An electronic money institution may take simplified due diligence measures if an electronic money device does not allow for reloading and the amount saved in one electronic money device does not exceed EUR250. [1] Credit and financial institutions supervised by Estonian Financial Supervision Authority may identify the client via electronic Estonian Identification Card if the value of the transaction(s) do not exceed EUR2,000 on a monthly basis. [1] Simplified due diligence measures may also be applied in a transaction if all of the following conditions have been fulfilled: a) a written contract has been entered into with a customer for an indefinite period; b) a payment is made through the account of a customer or a person participating in a transaction, which has been opened in a credit institution or a branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution which has been registered or has its place of

		business in a contracting state of the EEA or in a country where requirements equal to those provided for in Estonian legislation are in force; c) the obligated person has established by rules of internal procedure beforehand that the annual total value of performance of financial obligations arising from transactions of such type does not exceed the maximum limit of EUR15,000; and d) the obligated person registers at least the data specified in A10 with regard to a customer. Certain other criteria exist for applying simplified due diligence measures for public/state institutions (both local and foreign).
	In what circumstances are enhanced customer due diligence measures required?	a) if the nature of a situation involves a high risk of money laundering or terrorist financing; b) if a person participating in a transaction, in a professional operation, or using a professional service; or a customer has been identified and verified without being present at the same place as the person or customer; c) if upon identification or verification of a person suspicion arises regarding the truthfulness of the data or authenticity of the documents submitted or regarding the identification of the beneficial owner or beneficial owners; and d) if a subject is a politically exposed person of a contracting state of the European Economic Area or a third country or their family member or close associate.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Upon establishment of a business relationship with or entry into a transaction with or performance of a professional operation for or provision of professional services.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	The regular due diligence measures shall be applied more frequently than usually. Additionally, the following requirements must be implemented: a) appropriate risk-based internal procedures for making a decision on establishment of a business relationship or entry into a transaction applied; b) the management board or a person or persons authorised by the management board shall decide on establishment of business relationships; and c) upon establishment of a business relationship and entry into a transaction, appropriate measures taken for identification of the origin of the money or other property used. Also at least one of the following enhanced due diligence measures shall be undertaken: a) identification and verification of a person on the basis of additional documents, data or information, which originates from a reliable and independent source or from a credit institution or a branch of a credit institution registered in the Estonian commercial register or from a credit institution which has been registered or has its place of business in a contracting state of the EEA or in a country where requirements equal to the Estonian legislation are in force, and if in such credit institution the person has been identified while being present at the same place as the person; b) application of additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be notarised or officially authenticated or confirmation of the correctness of the data by the credit institution which issued the document; and c) making the first payment relating to a transaction through an account opened in the name of a person or customer participating in the transaction in a credit institution which has its place of business in a contracting state of

		the EEA or in a country where requirements equal to those provided for in Estonian legislation are in force. Also enhanced due diligence measures shall be undertaken upon opening a correspondent account with a credit institution of a third country and during the period of validity of the respective contract, thereby regularly assessing the following: a) based on public information, the nature of the economic activities and the trustworthiness and reputation of the credit institution of the third country and the effectiveness of supervision exercised over the credit institution; and b) the control systems of the credit institution of the third country for prevention of money laundering and terrorist financing. The contract serving as the basis for opening a correspondent account or the rules of procedure of the credit institution shall contain the obligations of the parties: a) upon application of due diligence measures for prevention of money laundering and terrorist financing, including with regard to a customer having access to a payable-through account or another similar account; b) upon submission, on the basis of a query, of data gathered in the course of identification of customers and verification of submitted information; and c) upon preservation of data and upon performance of the notification obligation and application of other measures for prevention of money laundering and terrorist financing. Prior consent of the management board of the credit institution or financial institution or the person authorised by the management board is required for opening a correspondent account for a credit institution or a financial institution of a third country or for opening a correspondent account in a third country credit institution or financial institution or for signing the corresponding contract. Credit institutions and financial institutions are prohibited to open or hold a correspondent account in a credit institution, which meets at least one of the following conditions: a) the actual place of management or business of the credit institution is located outside its country of location and the credit institution is not part of the consolidation group or group of undertakings of a credit institution or financial institution that is subject to sufficient supervision; b) an account for a credit institution corresponding to the characteristics specified in clause 1) has been opened in the credit institution; and/or c) according to international standards or the circumstances provided for in this section, which are to be used as a basis for assessment, deficiencies become evident in the trustworthiness of the executives of the credit institution and in assessment of measures for prevention of money laundering and terrorist financing.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Always, in the case of a person participating in a transaction, in a professional operation, or using a professional service; or a customer has been identified and verified without being present at the same place as the person or customer.

Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	An obligated person, except a credit institution, shall immediately, but no later than within two working days of executing the transaction, notify the Financial Intelligence Unit of any transaction where a financial obligation exceeding EUR32,000 is performed in cash, regardless of whether the transaction made is a single payment or several related payments. A credit institution shall immediately, but no later than within two working days of executing the transaction, notify the Financial Intelligence Unit of any currency exchange transaction exceeding EUR32,000 in cash, unless the credit institution has a business relationship with the person participating in the transaction. [1] [4]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Yes. External auditors must inform the Estonian Financial Supervision Authority if they find out that a credit institution materially violates Estonian law.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes: a) yes; b) corporate data is not protected under the data protection laws; and c) yes, sensitive personal data is: a. data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a legal person in private law registered pursuant to the procedure provided by law; b. data revealing ethnic or racial origin; c. data on the state of health or disability; d. data on genetic information; e. biometric data (above all fingerprints, palm prints, eye iris images and genetic data); f. information on sex life; g. information on trade union membership; and h. information concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter. Additional protections for sensitive personal data ("SPD"): a) written explicit consent has to be obtained from data subject; b) a person responsible for protection of personal data needs to be appointed or the processing of sensitive personal data registered with the Data Protection Inspectorate; and c) processing SPD for communication to third persons for assessing the creditworthiness or other such purpose is not permitted. [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	No.

FINLAND		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes. Guidance is provided by the Money Laundering Clearing House of Finland which operates within the National Bureau of Investigation ("NBI") (https://www.poliisi.fi/en/national_bureau_of_investigation). [1] [4]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	There is no minimum Euro threshold for taking customer due diligence measures. Customer due diligence must be followed when transactions are unusual. Due diligence must take place if one of the following is true: a) if the reporting entity is planning to engage in a permanent business relationship with a customer; b) if the transaction or transactions related to the same business amounts to EUR15,000 or more and the relationship between the reporting entity and a customer is occasional; [1] [5] c) if the customer is a gambling service provider; d) if the transaction is suspicious or the reporting entity is suspecting that the money related to the transaction is used to finance terrorism; or e) if the reporting entity is questioning the reliability of the information previously used to identify the customer.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: Full name, date of birth, identification number (for foreign citizens: citizenship and passport number). Required documents for individuals: passport, driving licence or official identity card. Legal entities: Name, business identification number, date of registration (and name of registration authority), field of activity as well as full name, date of birth and citizenship of members of the statutory bodies and the person(s) representing the legal entity. Required documents for legal entities: trade register extract or equivalent official extract from a relevant public register and relevant documents for the individuals previously mentioned.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	A certified copy signed by two qualified individuals is required. The qualified individual does not have to be a notary, lawyer or accountant.
	In what circumstances are reduced/simplified due diligence arrangements available?	Reduced/simplified due diligence arrangements are available if the risk of money laundering or the financing of terrorism connected to the customer, product, service or field of activity is low. For example, simplified due diligence arrangements are available to: a) Finnish authorities; b) public companies listed on the Finnish or any other European Economic Area ("EEA") country exchange; c) credit institutions; d) financial institutions; e) investment firms; f) management companies/custodians; and g) insurance companies with concession in Finland or another EEA country.

	In what circumstances are enhanced customer due diligence measures required?	Enhanced due diligence measures are required if there is a high risk of money laundering or the financing of terrorism in connection to the customer, product, service or field of activity. Enhanced due diligence is also required if the transaction is connected to a state in which systems for preventing and clearing money laundering does not meet international standards.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Additional due diligence is required if the customer himself is a PEP or is related to a PEP, or is an individual who is known to be the business partner of a PEP.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Firstly, the management of the credit institution has to approve the correspondent banking relationship. Should it be approved, the credit institution has to collect sufficient information about the correspondent bank which includes evaluating the bank's reputation, the quality of its supervision and the correspondent bank's measures to prevent money laundering and the financing of terrorism.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Additional due diligence is always required if the customer is not physically present for identification.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	If customers do not provide the information required for performing customer due diligence or if parties subject to the reporting obligation consider that the information provided is not reliable, the parties must make a suspicious transaction report. A suspicious transaction report must also be made if legal persons cannot be identified or their beneficiaries cannot be established in a reliable way, or if enhanced identification of the person for whom a customer is acting is not possible.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	a) yes, the definition of personal data covers any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household; b) the definition of personal data also covers personal information in the corporate context; and c) yes, "sensitive data" is defined as personal data related to or intended to be related to for example race or ethnic origin, the social, political or religious affiliation or trade-union membership of a person, a criminal act, punishment or other criminal sanction, the state of health, illness or handicap of a person or the treatment or other comparable measures directed at a person, the sexual preferences or sex life of a person or the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person. As a main rule, the processing of sensitive data is prohibited but Finnish law provides certain detailed derogations from the prohibition.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Yes, EU Data Protection Directive 95/46/EC and legislation based on the implementation of the said Directive apply when personal data is transferred from another EU country. If the information is transferred from outside of the EU, local legislation may be applicable. Personal Data Act (523/1999) is applicable on personal data and as special legislation may be applicable, for example Act on the Protection of Privacy in Working Life (759/2004), Employment Contracts Act (55/2001), Act on Cooperation within Undertakings (725/1978), Occupational Safety and Health Act (738/2002) Credit Data Act (527/2007) and other legislation. [1]

FRANCE		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes, guidelines have been provided by ACPR on various topics: a) business relationships and occasional customers; b) beneficial ownership; c) third party introduction; d) exchange of information within a group and non-group; e) reporting suspicious activity; f) politically exposed persons; g) wealth management; h) equivalent third countries; and i) suspicious reports to FIU. Application principles have been published on the ACPR website relating to: a) collective investment schemes; b) correspondent banking; c) transfer of funds; d) insurance sector; and e) insurance third party introduction. Guidelines have been provided by AMF for entities subject to its control (asset management companies and management companies, financial investment advisers, central security depositaries): a) obligation of vigilance in a risk based approach and conditions for implementation of obligation to report to Tracfin; b) Politically Exposed Persons ("PEPs"); c) conditions for implementing specific legislative and regulatory provisions; d) beneficial ownership; and e) third party introduction. Sources of practical guidance includes: a) (http://acpr.banque-france.fr/en/prudential-supervision/amlcft-anti-money-laundering-and-counter-terrorist-financing.html); b) (http://www.amf-france.org/en_US/Reglementation/Doctrine/Doctrine-list/Doctrine.html?category=III+-+Providers&docId=workspace%3A%2F%2FSpacesStore%2Fc59ace50-a95b-4f9e-990f-6433f6405808&docVersion=1.3&langSwitch=true); c) (http://www.economie.gouv.fr/tracfin); d) (http://www.fbf.fr/fr/environnement-europeen-et-international/lutte-anti-blanchiment/_875GT2&Count=8); and e) (http://www.arjel.fr/-Textes-de-reference-.html). [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes. The identification of occasional customers and beneficial owners is not required for transactions under EUR15,000 (and EUR1,000 for remitter) if the transaction is not deemed suspicious. However, this threshold is not applicable for money transfers, custody services when the client is not physically present. The decree of 28 Feb 2013 provides that under certain conditions, the identification of customers and beneficial owners may not be checked for online operations under EUR250 or for a total of EUR2,500 in one year. The decree of 07 May 2013 provides that for money transfers, information concerning the customer and the beneficial owner must be reported to Tracfin (see A18) for transactions over EUR1,000 or which cumulate over EUR2,000 on a calendar month. [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: a government-issued document with a photograph (such as a valid passport or a valid photocard driving licence), supporting documents of home address at the date when the documents are collected, occupation, revenues or any other relevant documents which enable the client's resources and his personal assets to be assessed Legal entities: original or certified copy of any deed or extract of an official register stating the company name, address, legal status and identity of the executives, annual reports of the last 3 years and auditors' reports.

	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Individuals: Original identification documentation must be provided. A bank's employee is required to make a copy of the original documentation and certify it true to the original. Legal entities: Except in the specific case of the presentation of a certified copy of a deed or extract of an official register stating the name, legal form and registered office, original documentation should be provided and a copy shall be made and certified by the bank's employee.
	In what circumstances are reduced/simplified due diligence arrangements available?	Due diligence may be reduced when the money laundering risks associated with a given customer and/or business relationship are considered as low. Low risk customers include: a) financial institutions subject to equivalent AML regulation; b) large corporates whose shares are listed on a regulated stock-exchange incorporated in an EU-country or an equivalent third-party country; and c) public administrative bodies or authorities of an EU country. Low risk products include life insurance contracts with an annual premium under EUR1,000 or with a unique premium under EUR2,500. Furthermore, the decree of 28 Feb 2013 provides that under certain conditions, the identification of customers and beneficial owners may not be checked for online operations under EUR250. [4] [1]
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence measures are required in the following cases: a) when the client or his representative is not physically present for the account opening; b) when the client is a Politically Exposed Person; c) when the transaction or the financial instrument facilitates the anonymity of the client; d) when the transaction is carried out by individuals who live or corporates which are incorporated in non-cooperative countries; and e) when the transaction is complex, of an unusual amount or without obvious justification.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Enhanced due diligence is systematically required for non-resident PEPs (with the fourth directive resident PEP will be concerned)
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Institutions must: a) collect sufficient information on its correspondent banking relationships' activities and assess, based on publicly available information, its reputation; b) assess its anti-money laundering arrangements; c) ensure that the decision of establishing this relationship has been approved by an executive of the institution; d) include in the correspondent-banking agreement the requirements to provide the institution with information on demand; and

		e) ensure that the correspondent-banking counterparty has checked the identity of its clients when the institution has opened accounts which are directly used by the correspondent-banking clients for their own transactions. Guidelines have been provided by the ACPR on the requirements around correspondent banking relationships: (http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201303-ACP-Principes-d-application-sectoriels-sur-la-correspondance-bancaire.pdf) [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Regulation requires institutions to systematically conduct enhanced due diligence for non face-to-face transactions and/or relationships.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Yes: a) operations which are particularly complex, an amount which appears to be unusually high or does not appear to have any economic justification, where the bank is unable to establish the identity of the beneficiary or obtain sufficient information regarding the origin and destination fund, the commercial background or the legality of a transaction; b) transactions for which the identity of the originator or the beneficiary could not be established; and c) for money transfers, transactions over EUR1,000 operations or which cumulate EUR2,000 on a calendar month.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No, but regulation relating to internal control provides that the AML policy should be described and communicated to the audit committee. In addition, a questionnaire is completed on an annual basis concerning AML internal control set up for the ACPR.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	In France, personal data is protected by the law on data processing, data files and individual liberties dated 01 Jan 1978: a) yes; b) corporate data include personal data concerning individuals representing legal entities. The collection and processing of these data are provided in the French law. These data can be collected and transferred for AML purposes (e.g. power of attorney, delegation of authority, identity of directors, officers and shareholders); and c) under French law, sensitive data is any personal data that reveals directly or indirectly racial or ethnic origins, political, philosophical or religious opinions, trade union membership or data related to individual health or sexual life. The collection of sensitive data is prohibited. By exception, sensitive data can be collected with the explicit consent of the person concerned or if the treatment of such data is required for public interest purposes.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Under French law, the transfer of information is governed by: a) the law on data processing, data files and individual liberties dated 06 Jan 1978; and b) the rules related to banking and professional secrecy. These rules aim at protecting the transfer of information and limit it to specific cases.

GREECE		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	The Competent Authorities have issued Interpretative Circulars, Decisions and Regulatory Acts, each one giving instructions and interpretations of the AML provision to the obligated persons under their supervision. The Competent Authorities through such Decisions / Acts have the power to modify the obligations laid down in the Greek AML legislation for the Obligated Persons.
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes. In principle, occasional (one-off) transactions below EUR15,000; a lower threshold of EUR1,000 per insurance contract per year (or of EUR2,500 in the case of a one-off payment). The law also caters for a lower threshold option in relation to electronic funds transfers depending on the decision and guidance provided by the respective regulatory authority.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: For identifying individuals, a police identity card or passport plus any other document that provides evidence of his/her residential and business address, as well as his/her profession and tax registration number. Legal Entities: Most recent legal documentation as defined by Greek law depending on the type of entity, identifying: a) business name, address and purpose of the entity; b) representation and signing authorities of the entity; c) any changes and amendments on the statutes of the entity and/or its representatives; d) police identity cards or passports of the legal representative(s) of the entity as well as evidence of their current residence; e) tax registration number; and f) Beneficial Owner(s). Notwithstanding the above, and specifically for credit and financial Institutions, the Bank of Greece Governor's Act No. 2652/29.2.2012 and article 68 para.7 of L. 4174/2013, as in force, determined that the customer's income shall be verified through the customer's income tax clearance form or, in the case of legal persons, the income tax returns filed (including confirmation of their filing that includes the tax payable), with the exception of the cases where the customer is exempted from the obligation to file income tax returns in accordance with the relevant provisions of the Income Tax Code, as in force.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Copies of identification documents may be certified by a state authority, a notary public or a lawyer. Copies may also be certified by an authorised employee of a financial institution upon presentation of the originals. In specific for the obligated persons under the supervision of the Hellenic Capital Market Commission ("HCMC") it has been recently decided that the certification documents of their clients which have been categorised as high risk and having a capital for investment exceeding the amount of EUR75,000 should be authenticated by a public authority, or an EU bank, or other bank of a country applying the FATF recommendations (art 2. para.10 of HCMC Decision 1/506/8.4.2009). [1]
	In what circumstances are reduced/simplified due diligence arrangements available?	Under local legislation it is up to the discretion of the relevant party to decide not to perform identity checks (unless there is a suspicion of money laundering) for credit and financial institutions or organisations situated in the EU or in a third country which impose requirements equivalent to those

		laid down in Directive 2005/60/EC and are supervised for compliance with those requirements. In addition, there are reduced due diligence requirements (no verification requirement) for other types of entities such as: a) listed companies whose securities are admitted to trading on a regulated market in one or more Member States which are subject to disclosure requirements consistent with Community legislation; b) companies operating as undertakings for collective investment in transferable securities and are based in the European Union and operate in consistency with the provisions of Directive 85/611/EEC as currently in force; c) Greek public law legal entities and state owned organisations of at least 51%; and d) public authorities or public bodies which satisfy certain requirements. Moreover, there are reduced due diligence requirements (no verification requirement) for: a) life insurance policies where the annual premium is no more than EUR1,000 or the single premium is no more than EUR2,500; b) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; c) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; and d) electronic money, where the maximum amount stored in the device is no more than EUR250, or where, if the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR1,000 or more is redeemed in that same calendar year by the bearer. [1]
	In what circumstances are enhanced customer due diligence measures required?	On a risk-sensitive basis, enhanced customer due diligence measures are required, especially for: a) transactions without the physical presence of the customer; b) cross border correspondent banking; and c) politically exposed persons. Moreover, most of the Competent Authorities have issued guidance that the following type of customers should be considered as high risk for money laundering purposes and should be subjected to enhanced due diligence procedures: a) companies with bearer shares; b) offshore companies; c) non-profit entities or organisations;

		d) persons from countries that do not adequately implement FATF recommendations; e) trust or similar Foreign Law Entities; f) non-residents' accounts; g) portfolio management accounts of important clients; and h) business relationships and transactions that entail high risks related to tax evasion (this high risk category shall at least include: (i) Self-employed persons whose total income credited on their own accounts or on accounts of which they are the beneficial owners exceed EUR200,000 during the previous calendar year (ii) Legal persons whose total cash deposits or cash withdrawals exceed EUR300,000 during the previous calendar year). [1]
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	In all circumstances where PEPs are acting either as customers of obliged persons or beneficial owners of such customers.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, credit institutions shall: a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls; c) obtain approval from senior management before establishing new correspondent banking relationships; d) document the respective responsibilities of each institution; and e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Additional due diligence is required to mitigate the higher risk profile associated with non-face-to-face transactions. Where a customer approaches a firm remotely (by post, telephone or over the internet), the firm should have appropriate procedures to carry out non-face-to-face verification, either electronically or by reference to documents, by having in place additional verification checks to manage the risk of identity fraud. In this respect, obligated persons should take specific and adequate measures to counter the higher risk in cases where the customer is not physically present for identification purposes, mainly by applying one or more of the following measures: a) ensuring that the customer's identity is verified by additional documents, data or information; b) taking supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution based in the European Union; and c) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution based in the

		European Union. Obligated persons should pay special attention to any product or transaction which might favour anonymity and which, by nature or by virtue of information about the profile of the characteristic features of the customer, may be associated with money laundering or terrorist financing and take appropriate measures to avert this risk.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	There are Competent Authorities who have issued instructions to the obligated persons under their supervision for reporting, apart from suspicious transactions for money laundering and terrorist financing criminal activities (predicate offences, especially those connected with tax evasion) as well as unusual transactions / activities. Moreover, the Compliance Officers of certain Obliged Persons (including credit and financial institutions) are required to prepare a report, on an annual / bi-annual basis, providing considerable input for the assessment of the obliged person's compliance with the AML/TF provisions / policy with specific references in most cases to high risk clients / transactions. Such reports are assessed by the obliged persons' management (e.g. Board of Directors) and are submitted to the relevant Competent Authority in electronic form or in a hard copy. Credit Institutions, Payment Institutions and Electronic Money Institutions which have obtained license for establishment and operation in Greece as well as foreign Credit Institutions, Payment Institutions and Electronic Money Institutions which provide payment services (carry out transfer of funds) through established Greek branches or agents) are required to submit to the Competent Authority (Bank of Greece) on a regular basis, inter alia, data for the total number and amount of cross border transfer of funds from and to abroad (inbound and outbound funds), per country of payer's establishment (for inbound funds) or beneficiary's (for outbound funds) (Template I203, Bank of Greece Governor's Act 2651/20.1.2012, section I2, as in force). Moreover, Credit Institutions submit to the Bank of Greece, on a semi-annual basis, data and information relating to products, services and clients characterised as "high risk" in order that the ML and TF risk to which the Credit Institution is exposed be assessed (Template I204, Bank of Greece Governor's Act 2651/20.1.2012, section I2, as in force). In addition, credit and financial institutions are obliged (pursuant to article 15 para 4 of L. 4174/2013 and Min. Circular POL 1033/28.1.2014, as in force) to forward electronically to the Greek Ministry of Finance (General Secretariat of Information Systems) files with customer data having a financial and tax interest. This data, inter alia, cover: a) self-employed persons whose total income credited on their own accounts or on accounts of which they are the beneficial owners exceed the relevant amount set each time by Banking and Credit Committee Decision of the Bank of Greece (currently EUR200,000) during the previous calendar year; and b) legal persons whose total cash deposits or cash withdrawals exceed the relevant amount set each time by Banking and Credit Committee Decision of the Bank of Greece (currently EUR300,000) during the previous calendar year). [4] [5] [1]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Yes. Pursuant to the Bank of Greece Governor's ("BoCG") Act 2577/9.3.2006 as in force, such reporting is included in a relevant assessment report evaluating the adequacy of the bank's overall Internal Control Systems.

Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Greece has established data protection laws. The main piece of legislation is Law 2472/1997 which has implemented in all material respects the EU Directive 95/46. The definition of "personal data" in the data protection law covers material likely to be held for KYC purposes. Greek data protection law applies only to individuals and not to corporate data. There is a separate definition of "sensitive data" (art. 7 of law 2472/1997) which is in accordance with the definition/additional protections as set out by EU Directive 95/46 (article 8). [4] [5] [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Yes.

HUNGARY		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes, each regulator, indicated above in A3, issued guidance and/or template AML documents. Template policies are published by the supervisory bodies listed above on their websites.
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes - one-off transactions below EUR15,000 (other than where there are two or more such transactions which the firm believes are linked, and which together would amount to EUR15,000 or more) or any amount which is viewed to be of a suspicious nature.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	For the purposes of identification and verification procedures, service providers require the following documents to be presented: Natural persons: a) personal identification document (official identity card) and official address card of Hungarian citizens; and b) passport or personal identity card for foreign nationals or documentary evidence of the right of residence or a valid residence permit. Legal persons and business associations: a) the application for registration or the document of registration for recognised legal persons, or the articles of incorporation of legal persons and business associations lacking legal status whilst not

		yet registered by the registrar of companies, court or appropriate authority; and b) for non-resident legal persons and business associations lacking the legal status of a legal person, the document proving that the person or body has been registered under the law of the country in which it is established.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Certified copies of the documents shall be accepted for identification procedures if certified by the competent authority of the country where it was issued or by the competent Hungarian foreign representative. Certified copies of the documents referred to above shall be accepted for the verification of the identity of the customer if: a) it was prepared by the officer of a Hungarian consular post or by a notary public and certified accordingly; b) the officer of a Hungarian consular post or the notary public has provided an endorsement for the copy to verify that the copy is identical to the original presented; or c) the copy was prepared by an authority of the country where it was issued, if such authority is empowered to make certified copies and the competent Hungarian consulate officer has provided a confirmatory certification of the signature and seal of the authority.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified customer due diligence applies where the customer is: a) a service provider engaged in carrying out the activities defined in the law (financial services, investment services, insurance services, commodity exchange, postal financial intermediation services and voluntary mutual insurance fund services) in the territory of the European Union (“EU”), or a service provider that is engaged in these activities and situated in a third country which imposes requirements equivalent to those laid down in the Money Laundering Act; b) a listed company whose securities are traded on a regulated market in one or more member states, or a listed company from a third country that is subject to disclosure requirements consistent with European Community legislation; and c) a supervisory body mentioned in the law/central government body or a local authority/a body of the European Community. Simplified customer due diligence also applies for insurance policies with a low-level annual/single premium and insurance policies for pension schemes if there is no surrender clause and where the funds payable to the insured person cannot be used as collateral for any credit or loan arrangement. An insurance company shall not be required to apply customer due diligence measures for identifying a customer whose identity has already been established by an independent insurance intermediary for the same purpose. [1]
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence is applicable for: a) customers that have not been physically present for identification purposes or the verification of their identity; b) correspondent banking relationships; c) PEPs; and

		d) transactions for the exchange of money involving a sum of EUR2,000 or more. The service provider will record further information pertaining to the business relationship and the transaction order e.g. the type, subject matter and term of the contract of the business relationship and the subject matter and the value of the transaction order.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Customers residing in another member state or in a third country are required to provide a statement as to whether they are considered politically exposed according to the national law of their country. In respect of transactions or business relationships with PEPs residing in another member state or in a third country, approval from the management body, as defined in the organisational and operational regulations, is required.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Service providers engaged in the provision of financial services or in activities auxiliary to financial services are required, before establishing correspondent banking relationships with respondent institutions from third countries to: a) assess, evaluate and analyse the respondent service provider's anti-money laundering and anti-terrorist financing controls; b) be satisfied that the respondent service provider has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to monitor access to the accounts of the correspondent on an ongoing basis; and c) be satisfied that the respondent service provider is able to provide relevant customer due diligence data to the correspondent institution, upon request. Approval from the management body must be obtained to engage in correspondent banking relationships. [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Reporting entities are required to consider the additional risk posed by non face-to-face business in accordance with the risk based approach and procedures they have adopted. Service providers are required to record all data and particulars specified in the law, where the customer has not been physically present for identification purposes or for the verification of his identity.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	No.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Service providers under the AML Act are required to incorporate details on their AML systems and controls in their internal AML policies. The policies are not subject to reporting but can be reviewed by the FIU upon inspection.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data?	Act 112 of 2011 on information governance and information freedom regulates the issues of personal data protection: a) yes. Personal data is any data that can be connected to the individual, especially the name, any identification codes or numbers, or one or more pieces of information on the physical, physiological, mental, economic, cultural or social identity, and further any consequences that can be drawn therefrom;

	c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	b) the same rules apply as long as the corporate data contains any individual's personal data, otherwise, corporate date is not subject to any special protection; and c) sensitive data are called special data in Hungarian terms. These are any personal data that refer to race, nationality, political views, party connections, religion or other religious beliefs, any memberships and sexual life. Furthermore, all personal data on health status and addictions and criminal records. The latter may only be controlled with the written consent of the individual. [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	The AML Act itself regulates the transfer of information.

IRELAND		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Industry guidance notes have been prepared by a committee representing various sectors of the financial services industry. The Core Guidelines have been drafted jointly by various sectors of the financial services industry. The guidelines are stated to be for the purpose of guiding designated persons on the application of Part 4 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. While these guidelines have not been approved under Section 107 of the Act, the Central Bank will have regard to these guidelines in assessing compliance by designated persons with the Act. Links to the various guidelines can be located via: http://www.finance.gov.ie/viewdoc.asp?DocId=-1&CatID=16 [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	In relation to "occasional transactions" where the total amount of money paid by the customer in a single transaction or series is greater than EUR15,000.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	The CJA 2010 specifies in section 33(2)(a) that the measures to be applied under section 33(1) of the Act include identifying the customer, and verifying the customer's identity on the basis of documents (whether or not in electronic form), or information that the designated person has reasonable grounds to believe can be relied upon to confirm the identity of the customer, including: a) documents from a government source (whether or not a State government source); or b) any prescribed class of documents, or any prescribed combination of classes of documents. The Guidance states that the following information should be obtained and verified: Individuals: Name, Date of Birth and Current Address.

		Documentary Verification: "One plus One" approach – one item from the list of photographic IDs (typically to verify name and date of birth) and one item from the list of non-photographic IDs (typically to verify address). Photographic ID: a) current valid passport; b) current valid driving licence; and c) current valid National Identity Card. Non Photographic ID: a) official documentation / cards issued by the Revenue Commissioners and addressed to the individual; b) official documentation / cards issued by the Department of Social and Family Affairs and addressed to the individual; c) instrument of a court appointment (such as liquidator, or grant of probate); d) current local authority document e.g. refuse collection bill, water charge bill (including those printed from the internet); e) current statement of account from a credit or financial institution, or credit/debit card statements (including those printed from the internet); f) current utility bills; (including those printed from the internet); and g) current household/motor insurance certificate and renewal notice. Legal persons: Name, legal form and proof of existence, address of registered office and main place of business, the nature of the business and its ownership and control structure) and directors or equivalent (either two directors or one director and one authorised signatory) and beneficial owner(s) to be verified as warranted by the risk. Documentary verification: a) a search of the relevant company or other registry; b) a copy, as appropriate to the nature of the entity, of the certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust or other official documentation proving the name, form and current existence of the customer; c) in cases regarded by the Designated Person as higher risk, use of more than one source of information may be warranted; and/or d) obtain a copy of the annual audited accounts listing directors. [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	The Guidance states that the following, and potentially their equivalents in other jurisdictions, are considered suitable persons to certify documentation, where they are willing to do so: a) Garda Siochana / Police Officer;

		b) Practising Chartered & Certified Public Accountants; c) Notaries Public / Practising solicitors; d) Embassy / Consular Staff; e) Regulated financial or credit institutions; f) Justice of the peace; g) Commissioner for oaths; or h) Medical professional.
	In what circumstances are reduced/simplified due diligence arrangements available?	Specified Customers: a) credit and financial Institutions; b) listed companies; c) public bodies; and d) beneficial owners of Pooled Accounts held by Solicitors and other Legal Professionals. Specified Products: a) electronic money (the device cannot be recharged, the maximum amount stored in the device is no more than EUR250 or EUR500, if the device cannot be used outside the State. Where the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except where an amount EUR1,000 or more is redeemed in that same calendar year by the bearer of electronic money); [1] b) life assurance policy (having an annual premium of no more than EUR1,000 or a single premium of no more than EUR2,500); and [1] c) pensions.
	In what circumstances are enhanced customer due diligence measures required?	Enhanced due diligence is required in respect of: a) a correspondent banking relationship; b) a business relationship or transaction with a non-resident PEP; and c) a higher risk customer (including non-face to face).
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	The CJA 2010 requires designated persons to apply enhanced measures to PEPs that are resident outside the State but not to domestic PEPs (under the definition of a PEP, an individual ceases to be so regarded one year after he has left office).
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Section 38(1) of the CJA 2010 states that prior to commencing the relationship, the credit institution: a) has gathered sufficient information about the respondent institution to understand fully the nature of the business of that institution; b) Is satisfied on reasonable grounds, based on publicly available information, that the reputation of the respondent institution and the quality of

		supervision or monitoring of the operation of that institution in the place are sound; c) is satisfied on reasonable grounds, having assessed the anti-money laundering and anti-terrorist financing controls applied by the respondent institution, that those controls are sound; d) has ensured that approval is obtained from the senior management of the credit institution; and e) has documented the responsibilities of each institution in applying anti-money laundering and anti-terrorist financing controls to customers in the conduct of the correspondent banking relationship. [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Section 33(4) of CJA 2010 contains a supplementary obligation on a designated person where a customer who is an individual does not present in person. This is not an alternative obligation but a supplementary one. The subsection provides that, without prejudice to the generality of section 33(2)(a), one or more of the following measures shall be applied by a designated person under section 33(1) of the Act, where a customer who is an individual does not present to the designated person for verification in person of the customer's identity. e.g. verification of the identity with additional documentation; robust anti-fraud checks, etc.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Section 43 CJA 2010 requires a relevant person to report any service or transaction which is connected with a place that does not have adequate procedures in place for the detection of money laundering or terrorist financing (the power to designate a jurisdiction is contained in section 32 CJA 2010).
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes: a) yes; b) the laws apply to Personally Identifiable Information ("PII") but not to other aspects of Corporate Data; and c) yes, sensitive data includes Personally Identifiable information and other sensitive personal data, such as medical records. Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Sensitive personal data means personal data as to: a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject; b) whether the data subject is a member of a trade union; c) the physical or mental health or condition or sexual life of the data subject; d) the commission or alleged commission of any offence by the data subject; or e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Additional rules apply regarding transfer of data to third countries (i.e. those outside the European Economic Area EEA). The rules regarding transfers to third countries can be summarised as follows:

		a) the general rule is that personal data cannot be transferred to third countries unless the country ensures an adequate level of data protection. The EU Commission has prepared a list of countries that are deemed to provide an adequate standard of data protection; b) if the country does not provide an adequate standard of data protection, then the Irish data controller must rely on use of approved contractual provisions or one of the other alternative measures, provided for in Irish Law; and c) the Data Protection Commissioner retains the power to prohibit transfers of personal data to places outside of Ireland, if he considers that data protection rules are likely to be contravened, and that individuals are likely to suffer damage or distress as a result.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Yes, EU laws apply - EU Data Protection Directive (95/46/EC).

ITALY		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes, guidelines for Organisation and Internal Controls for AML purposes and Guidelines for KYC rules for the Banking and Financial sector.
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, one-off transactions below EUR15,000 (other than where there are two or more such transactions which the firm believes are linked and which together would amount to EUR15,000 or more) and EUR1,000 for cash and bearer instruments.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Any person who: a) opens, changes or closes a current, savings or deposit account or has another 'continuing relationship'; or b) carries out a single transaction, or several transactions which appear to be linked, involving the transmission, handling or the transfer of means of payment or bearer instruments in an amount of EUR15,000 or more; must be identified and must indicate in writing the full details of the person, if any, on whose behalf the transaction is carried out. Identification must take place each time a transaction is executed. [1] Individuals: evidence of identity should be obtained such as name, address, date and place of birth, tax code and a government issued document e.g. an identity card, passport or driving licence. Legal persons: evidence of the identity of the firm, as well as the identity of the person physically present at the transaction, should be obtained such as the company name, registrar office, tax code and evidence of the identity of the beneficial owner.

	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Financial institutions, designated non-financial businesses and professionals cannot rely on a copy of an identification document. An exception is provided for copies validated by public officers.
	In what circumstances are reduced/simplified due diligence arrangements available?	Other than for telephone and internet banking, there are specific provisions allowing for simplified due diligence. Customer due diligence is not required in the following cases: a) transactions and account relationships between equivalent financial institutions; b) the transfer of funds within the State Treasury and payments arranged by the public administration, through the State Treasury, with the exception of payment operations linked to the national debt; c) the accounts, deposits and other continuing relationships between provincial sectors of State treasuries, the Bank of Italy and the Financial Intelligence Unit ("FIU"); d) relationships and transactions between banks, other licensed intermediaries that have their head office or branch in Italy and banks or branches located abroad. This exemption applies regardless of whether the countries in which the banks/branches are located have effectively implemented the FATF Recommendations; and e) when the customer is a listed company.
	In what circumstances are enhanced customer due diligence measures required?	There are specific provisions requiring enhanced due diligence for higher risk categories of customers (for example PEPs), operations or transactions such as financial products distributed via the internet (or when the customer is not physically present), companies incorporated in a tax haven or a country listed on the Organisation for Security and Co-operation in Europe ("OSCE") grey list.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Article 28(5) of Legislative Decree 231/2007 requires the application of enhanced due diligence measures to foreign PEPs which comprise: a) establishing adequate risk-based procedures to determine whether the customer is a politically exposed person; b) obtaining the authorisation of the general manager, his delegate or a person performing an equivalent function before establishing a continuous relationship with such customers; c) taking all necessary measures to establish the source of wealth and source of funds that are involved in the continuous relationship or the transaction; and d) conducting enhanced ongoing monitoring of the continuous relationship or professional service. [1]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	For correspondent banking relationships, banks, financial and non financial institutions as well as professionals have to perform enhanced due diligence and acquire information as provided by the public register. In addition, where possible, they must evaluate the internal control system of their correspondent bank and can only start the business relationship with the authorisation and responsibility of senior management.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	The 'Decalogo' of the Bank of Italy requires financial intermediaries to adopt special precautions for transactions relating to telephone or electronic accounts, and to take steps to ensure adequate knowledge of the customer and his business in cases of relationships with customers in non face-to-face situations.

Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	There is an obligation to report all financial transactions above EUR3,000 made by credit card or e-payment, but this is not specifically for AML purposes. This type of report is made to the tax agency (Agenzia delle Entrate). [1]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	There is a general requirement for auditors to report on the bank's systems and internal controls.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	a) yes; b) N/A; and c) N/A.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	N/A

LATIVA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Control service (http://www.prokuratura.gov.lv/public/29881.html) (in Latvian; information on Control Service (Kontroles dienests)). Practical guidance for certified auditors (www.lzra.lv), although please note this information is locked with a password. [1] [5]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	EUR15,000 (if there are no other indicators). [1] [4] [3]
	What are the high level requirements for verification of customer identification	Individuals: Latvian residents: document with name, surname and personal code. Non-residents: documents which allow the individual to be in Latvia, including a passport.

	information (individuals and legal entities)?	Legal entities: Registration documents, information of legal address, identity of representatives.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Originals should be provided.
	In what circumstances are reduced/simplified due diligence arrangements available?	A credit institution or financial institution registered in Latvia or EU Member State: a) a credit institution or financial institution registered in a country which complies with the EU requirements; b) a public municipal entity (ministry, city council, etc.) or a public or municipal capital company with inherently low money laundering; c) a merchant whose shares are traded in a regulated market in the EU or a third country in respect of which disclosure requirements that are similar to those of the EU exist; d) a person, in the name of which a public notary or a lawyer from the EU Member State or a country complying with the EU requirements; and e) a person with a low inherent money loundering risk (all the feature must be taken into account): a. the client has been engaged in public administration duties under the EU law; b. the information identifying the publicly available, transparent, reliable; c. the client's activities and accounting methods are transparent; and d. client business. [1] [4] [2]
	In what circumstances are enhanced customer due diligence measures required?	a) if the client was not participating in identification personally; b) for PEPs; and c) for cross border banking relations with respondents from third countries.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	For all transactions with PEPs, board approval is required along with risk-based actions to determine the origin of funds and the origin of well-being.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	a) obtaining the information on respondent for full understanding the nature of transaction, publicly available information about reputation and the quality of monitoring of the related bank or investment entity; b) evaluating AML actions undertaken by the respondent; c) receiving approval of the Board before establishing new correspondent relationships; and d) documenting respondent liability with regards to AML. Banks should ensure that they have no relationships with other financial institutions that are known to have transactions with shell banks.

	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	In all circumstances.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	a) unusual transactions; b) cash transactions over EUR60,000 for banks or over EUR40,000 for other entities; c) currency exchange transactions over EUR8,000 without the use of bank accounts; d) cash debited from the account immediately after crediting it; e) potential fraud; f) suspicious transactions abroad; and g) cash change over EUR2,000 (of one currency). [1]
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	N/A

LITHUANIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	N/A
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	One off transactions (single or linked) under EUR15,000 do not require customer due diligence. [10] [4]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: Full name, date of birth, identification number (for foreign citizens: citizenship and passport number). Required documents for individuals: passport, driving licence or official identity card. Legal entities: Name, business identification number, date of registration (and name of registration authority), field of activity as well as full name, date of birth and citizenship of members of the statutory bodies and the person(s) representing the legal entity. Required documents for legal entities: trade register extract or equivalent official extract from a relevant public register and relevant documents for the individuals previously mentioned. [10]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Originals should be provided.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence arrangements may be applied for: a) customers providing financial services, registered in EU or in equivalent country; b) central/local government entities or c) g) companies whose securities are admitted to public trading on a regulated market in at least one European Union member state or in an equivalent country. However, the institutions always need to take into account the risk of money laundering and terrorist financing.
	In what circumstances are enhanced customer due diligence measures required?	Enhanced due diligence procedures are required for PEP or Senior Foreign Political Figure
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	No enhanced due diligence procedures are required for domestic PEP. Enhanced procedures are required ONLY for foreign PEP / SFPF [10]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	For correspondent banking relationships, banks, financial and non-financial institutions as well as professionals have to perform enhanced due diligence and acquire information as provided by the public register. In addition, where possible, they must evaluate the internal control system of their correspondent bank and can only start the business relationship with the authorisation and responsibility of senior management.

	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Reporting entities are required to consider the additional risk posed by non face-to-face business in accordance with the risk based approach and procedures they have adopted.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	a) unusual transactions; b) potential fraud; c) suspicious transactions abroad
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes. Lithuania has established a data protection act. It has been in force since 21 Jan 2003 http://www.legislationline.org/documents/action/popup/id/5340 a) Yes b) the data protection law does not apply to corporate data as the definition of data subject does not include a company. Corporate data may be protected contractually by confidentiality agreements; c) No. [10] [4] [9]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	No.

LUXEMBOURG		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	A practical guide for the funds industry has been published by the Association of the Luxembourg Fund Industry ("ALFI"): http://www.alfi.lu//sites/alfi.lu/files/files/Alfi%20guidelines%20and%20recommendations/Guidelines-ABBL-ALCO-ALRIM-final.pdf [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, one-off transactions (single or linked) under EUR15,000 for occasional customers.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: Pursuant to Article 18 of the Regulation 12-02, the identity of a customer must be verified by means of a valid official document issued by a competent authority and bearing a photo and signature. In addition to passports and identity cards, other official documents such as residential permits can be accepted. Article 24 of the Regulation now clearly states that when establishing the client relationship, the information on the origin of funds must be part of this initial customer due diligence. Corporates: Articles of Association (or equivalent), extract of the Commercial Register (or equivalent), business authorisation if the entity manages funds of third parties, identification of the beneficial owners and of the persons with authorised signatures.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	If non face-to-face business is conducted, the copy should be certified as true by a competent authority, for example a consulate, embassy, police station or notary.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence arrangements are listed in Article 3-1 of the Luxembourg AML Law. Examples of simplified due diligence arrangements include: a) where the customer is a credit or financial institution subject to equivalent AML regulations and which is supervised; b) on certain conditions, pooled accounts held by notaries and other legal independent professionals; c) where the customer is a Luxembourg public authority; d) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; e) pension schemes that provide retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the transfer of rights; and f) where the customer is a listed company whose securities are admitted to trading on a regulated market within the meaning of Article 1-11 of the law of 13 Jul 2007 in one or more European Union ("EU") Member States or a listed

		company in a third country subject to disclosure requirements consistent with EU legislation. The new Grand-ducal regulation dated 05 Aug 2015 states in Article 2 simplified due diligence may be applied when online payment services fulfilling each of the following conditions are carried out: a) the transaction concerns the provision of payment services listed under number 3, second and third indents, number 4, second and third indent, number 5 and number 7 of the Annex to the law of 10 Nov 2009 on payment services, as amended; b) the transaction is executed via accounts held with payment service providers located in the EU or in a third country which imposes equivalent requirements relating to the fight against money laundering and terrorist financing; c) the transaction does not exceed a unit amount of EUR250; and d) the total amount of the transactions executed for the customer during the 12 months preceding the transaction does not exceed EUR2,500. It also applies to professionals with respect to electronic money referred to in Article 3-1(4)(d) of the Law of 12 Nov 2004.
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence measures are required in situations which by nature present a higher risk of money laundering or terrorist financing and at least in the cases listed in Article 3-2 of the Luxembourg AML Law (for example non face-to-face business, foreign PEPs and cross-frontier correspondent banking relationships with respondent institutions from non EU countries).
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Enhanced due diligence measures are required for foreign PEPs, including the implementation of an appropriate risk-based procedure to detect such foreign PEPs. Such measures should include senior management approval of customer acceptance, ascertaining the source of wealth/income and ensuring enhanced on-going monitoring of the relationship.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	For correspondent banking relationships and similar relationships, the correspondent bank must: a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; b) assess the respondent institution's AML and CTF controls; c) obtain approval from senior management before establishing new correspondent banking relationships; d) document the respective responsibilities of each institution; and e) with respect to payable-through accounts, be satisfied that the respondent credit institution has checked the identity of and performed on-going due diligence on the customers having direct access to the accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution upon request.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Enhanced due diligence measures are required for non-face-to-face customers. These include:

		a) obtaining additional documents, data or information that ensures adequate identification of customers; b) performing additional measures to verify or certify the identification documents (for example, copies of identification documents certified true by a credit or financial institution or by a competent authority); or c) first payment to be drawn on an account opened in the customer's name with a credit institution.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	No.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Yes.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes, the Law of 02 Aug 2002 on the protection of personal data transposes the EU Directive 95/46/CE: a) to the extent that KYC material includes information about individuals this falls within the definition of "personal data"; b) the Law does not cover corporate data but only personal data. Corporate entities related data are not in the scope of the Law; and c) no. The Law adopts the EU directive definition for data of a sensitive nature. In some cases, the processing of such data is prohibited; in other cases it requires an approval from the local Data Protection Authority.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	No.

MALTA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	The Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR") are supplemented by the Implementing Procedures issued by the FIAU (http://www.fiumalta.org/implementing-procedures). Sectorial procedures are also in place for the banking sector and land based casinos. [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	One off transactions (single or linked) under EUR15,000 do not require customer due diligence.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: The following information should be obtained: a) official full name; b) place and date of birth; c) permanent residential address; d) identity reference number, where available; and e) nationality. These should be verified against photographic evidence of identity listed through one of the following: a) a valid, unexpired passport; b) a valid, unexpired national identity card; or c) a valid, unexpired driving licence. The verification of the residential address shall be carried out by making reference to any one of the following documents: a) a recent statement from a recognised credit institution; b) a recent utility bill or any similar document as may be specified in sectoral implementing procedures issued by the FIAU; c) a correspondence from a central or local government authority, department or agency; d) a record of a visit to the address by a senior official of the subject person; or e) any government issued document listed above, where a clear indication of residential address is provided.

		Legal entity: The subject person is required to first identify the private company by gathering the following information: a) the company's official full name; b) the company's registration number; c) the company's date of incorporation or registration; and d) the company's registered address or principal place of business. These should be verified by viewing one or more of the following documents: a) the certificate of incorporation; b) a company registry search, including confirmation that the private company has not been, and is not in the process of being dissolved, struck off, wound up or terminated; or c) the most recent version of the Memorandum and Articles of Association or other statutory document. [4] [2] [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Certification of the documentation is required by: a) a legal professional; b) an accountancy professional; c) a notary; d) a person undertaking relevant financial business; or e) a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.
	In what circumstances are reduced/simplified due diligence arrangements available?	a) applicants for business, which are authorised to undertake relevant financial business, including regulated entities in the financial sector. This provision also applies to applicants for business which are licensed or authorised to carry out activities equivalent to relevant financial business in another Member State of the European Community or in a reputable jurisdiction; b) legal persons listed on a regulated market and which are subject to public disclosure requirements. These entities may either be authorised under the Financial Markets Act (42), an equivalent regulated market within the Community, or in a reputable jurisdiction; c) beneficial owners of pooled accounts held by notaries or independent legal professionals; d) certain domestic and foreign public authorities or bodies; and/or e) legal persons who present a low risk of ML/TF.
	In what circumstances are enhanced customer due diligence measures required?	The PMLFTR refer to three specific types of relationships in respect of which enhanced due diligence ("EDD") measures must necessarily be applied: a) where the applicant for business has not been physically present for identification purposes; b) in relation to cross-border correspondent banking relationships; and c) in relation to a business relationship or occasional transaction with a PEP.

	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Subject persons are required to apply EDD measures to all foreign PEPs as defined in the PMLFTR. Domestic PEPs need to be identified as such and EDD measures applied on a risk based approach. [1]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Where a credit institution seeks to establish such correspondent banking relationships it has to ensure that: a) it fully understands and documents the nature of the business activities of its respondent institution, including from publicly available information: a. the reputation of the institution; b. the quality of supervision of that institution; and c. whether that institution has been subject to a ML/TF investigation or regulatory measure; b) it assesses the adequacy and effectiveness of the internal controls of the institution for the prevention of ML/TF; c) it obtains prior approval of senior management; d) it documents the respective responsibilities for the prevention of ML/TF; and e) it is satisfied that, with respect to payable through accounts, the respondent credit institution has verified the identity of and performed ongoing due diligence of the customers having direct access to the accounts of the respondent institution and that it is able to provide relevant CDD data upon request.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Where the applicant for business has not been physically present for identification purposes, subject persons are required to apply one or more of the following measures: a) establish the identity of the applicant by using additional documentation and information; b) verify or certify the documentation supplied using supplementary measures; c) require certified confirmation of the documentation supplied by a person carrying out relevant financial business; and/or d) ensure that the first payment or transaction into the account is carried out through an account held by the applicant for business in his name with a credit institution authorised under the Banking Act or otherwise authorised in another Member State of the Community or in a reputable jurisdiction.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	a) subject persons shall examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions, including unusual patterns of transactions, which have no apparent economic or visible lawful purpose, and any other transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism, establish their findings in writing, and make such findings available to the Financial Intelligence Analysis Unit and to the relevant supervisory authority in accordance with applicable law. b) subject persons shall pay special attention to business relationships and transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity, from a jurisdiction that does not meet the criteria of a reputable jurisdiction as defined in regulation (2), and; where the provisions of sub regulation (1)

		apply to such transactions, subject persons shall proceed as provided for in sub regulation (1).
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes: a) in terms of the Data Protection Act (Chapter 440 of the Laws of Malta) ("DPA") the term 'personal data' means 'any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'; b) the DPA expressly provides that its provisions are to '...apply to the processing of personal data, wholly or partly, by automated means and to such processing other than by automated means where such personal data forms part of a filing system or is intended to form part of a filing system.' Hence, the DPA should apply to data which falls within the definition of 'personal data'. Furthermore, non-living entities should fall outside the scope of the DPA; and c) the DPA defines the term 'sensitive data' as '...personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life'. The general rule is that sensitive personal data may only be processed if the data subject: a. has given his explicit consent to processing; or b. has made the data public.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	There are no known case law, laws or regulations that may impact upon the transfer of information to Malta. However, as noted on the Office of the Information and Data Protection Commissioner website (http://idpc.gov.mt/), the Commissioner is required to collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties, in particular by exchanging all useful information, in accordance with any convention to which is a party or other international obligation. Hence, bilateral agreements are in place with third countries for the transfer of data.

NETHERLANDS		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	a) (http://www.dnb.nl/en/home/index.jsp); b) (http://www.afm.nl/en); and c)(http://www.belastingdienst.nl/wps/wcm/connect/bldcontenten/belastingdienst/individuals/) and (www.bureauft.nl).
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, Customer Due Diligence is not required for business relationships leading to one or more transactions with a total value of less than EUR15,000.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: Verification of individual customer identification information includes: a valid passport, a valid Dutch identity card, a valid identity card issued by the competent authorities in another Member State and bearing a photograph of the holder indicating the holder's name, a valid Dutch driver's licence, a valid driver's licence issued by the competent authorities in another Member State and bearing a photograph of the holder indicating the holder's name, travel documents for refugees and aliens or aliens' documents issued pursuant to the Aliens Act 2000. Corporates: For the identification of Dutch legal persons: an (online) extract from the Chamber of Commerce/Trade Register; a deed or statement drawn up or issued by a lawyer, a civil-law notary, a junior civil-law notary or a comparable, independent legal professional resident in the Netherlands or in another Member State; a document showing that a religious community, or a religious body in which it is united, is affiliated with the Interchurch Contact in Government Affairs (Interkerkelijk Contact in Overheidszaken) or that the religious community or religious body has been designated as an institution as referred to in section 6.33(1)(b) of the Income Tax Act 2001(Wet Inkomstenbelasting 2001); a document showing that an independent section of a religious community forms part of that religious community and the religious community fulfils the statutory provisions. [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	If documents do not originate from public authorities or the courts, the institution will question if the documents are sufficiently reliable. Usually, such documents will, in and by themselves, be insufficient to verify identity in an adequate manner.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence arrangements are available for customers with a specific legal personality and a very technical and detailed set of products.
	In what circumstances are enhanced customer due diligence measures required?	Based on the risk profile of the customer, transaction, product or country concerned, enhanced due diligence must always be carried out if: a) the customer is not physically present; b) the customer is a PEP; c) there is a correspondent banking relationship; or d) if facts or circumstances, including the country where the customer lives or is established, suggest a higher risk of money laundering or terrorist financing.

	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Enhanced due diligence measures are required in the case of transactions or business relationships with PEPs who live in a different country or Member State (regardless of their nationality), or who live in the Netherlands with a non-Dutch nationality.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Enhanced due diligence is required for all correspondent banking relationships outside the EU, whereby a number of factors need to be taken into account including, but not limited to: a) obtaining sufficient information to obtain a full picture of the nature of the bank's activities; b) evaluation of the reputation of the bank and quality of oversight based on publicly available information; and/or c) evaluation of procedures and measures to prevent money laundering and terrorist financing.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Identification in person is not obligatory in all circumstances. In summary, payment of services has to be done from a bank account. There are no additional requirements in local regulations or guidance. If identification cannot be done face-to-face this is regarded as high risk and is required to be adequately mitigated by enhanced due diligence.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Institutions with a duty to report are required to report unusual transactions. Guidance on objective and subjective indicators by industry sector which may indicate unusual transactions is provided on the FIU's website: http://en.fiu-nederland.nl/content/list-indicators
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	The Netherlands has an established Data Protection Act: Wet bescherming persoonsgegevens (Wbp: Dutch Data Protection Act). a) personal data is defined in a very broad manner in the Netherlands: "personal data shall mean: any information relating to an identified or identifiable natural person"; (art. 1 sub a. Wbp). It is therefore very likely that personal data held for KYC purposes is covered by this Act; b) art. 2 Wbp states: "This Act applies to the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein". Given the scope definition, corporate data is not covered by the Dutch Data Protection Act; and c) article 16 Wbp contains a prohibition on the processing of sensitive personal data (such as religion, race, political persuasion, health and criminal past), unless one of the exemptions listed in articles 17-23 Wbp apply. Pursuant to Article 23(1)f Wbp, the Dutch DPA may grant an exemption, if this is required in view of substantial general interest and appropriate guarantees are offered to protect personal privacy. [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	There are no specific restrictions on the transfer of personal data to the Netherlands. Transfer of data within the European Union: The Wpb does not have any individual provisions governing data movements within the European Union ("EU"), as the Wbp implements the European

		Directive for the Dutch jurisdiction. Data movement from the Netherlands to another EU Member State thus only has to conform to the general requirements of the Wbp. Transfer to countries outside the European Union: The Wbp has specific provisions for the movement of data to countries outside the European Union, the third countries (Chapter 11 Wbp). Third countries are all countries outside the European Union, with the exception of the countries of the European Economic Area ("EEA"). The countries of the EEA (Norway, Liechtenstein and Iceland) have undertaken to implement the directive in their own legislation. Appropriate level of protection: The primary rule is that personal data may only be transferred to a third country if the general requirements of the Wbp have been conformed to and the third country ensures an adequate level of protection. For a number of countries, the European Commission has adopted decisions regarding the adequacy of the level of protection. No adequate level of protection: If a third country does not provide an adequate level of protection, there are two possibilities for still being entitled to transfer data to these third countries: a) Transfer based on the exceptions mentioned in the Act (Art 77(1) Wbp); or b) Transfer based on a permit issued from the Minister of Justice. Such a permit will be made subject to additional conditions that serve as a guarantee for the protection of personal data. To apply for the permit, a form must be used. The granting of such a permit will be facilitated if the model contracts prepared by the European Commission are used for the transfer. [1]

POLAND		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	The Polish Banking Association ("ZBP") developed guidance concerning AML practices. The Regulator provides limited guidelines concerning AML procedures which are published on the website of the General Inspector of Financial Information.
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Any obligated institution shall apply financial security measures for its clients. Their scope is determined on the basis of risk assessment as for money laundering and terrorist financing, resulting from the analysis, taking into account in particular type of a client, economic relationships, products or transactions. There is no minimum threshold, under which customer due diligence is not required. However, any obligated institution, taking into account the risk of money laundering or terrorist financing, may waive the above for: a) life insurance policies, where an annual premium shall not exceed the equivalent of EUR1,000, or a single premium shall not exceed the equivalent of EUR2,500; and

		b) electronic money, if: – the maximum amount stored in the device does not exceed the equivalent of EUR250 - in the case of a device that cannot be recharged – the maximum amount of transfers of electronic money does not exceed the equivalent of EUR2500 per calendar year in question – unless the redemption amount of electronic money shall be at least equivalent of EUR1,000 per calendar year in question. [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: Determining and noting the distinguishing features of a document confirming the person's identity pursuant to separate regulations, or of a passport, as well as the first name, last name, the citizenship and address of the person executing the transaction, and furthermore the PESEL (national citizens' registry) number in the case of the identification on the basis of identity card or date of birth for a person without a PESEL number, number of ID for foreigners and country code in the case of the passport. Legal entities: Up-to date information from a court registry extract or other document specifying its name, the organisational form of the legal entity, its location, address and tax ID number, as well as the name, surname and PESEL or date of birth of the person executing the transaction to represent the legal entity.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Not stated in local regulations or guidance regarding external third party certification. Certification of copies of identification documents may be made by a state authority, a notary public or a lawyer.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence arrangements may be applied for: a) customers providing financial services, registered in EU or in equivalent country; b) central/local government entities; c) life insurance arrangements (if year contribution is less than EUR1,000 or one-time contribution is less than EUR2,500); d) insurance policy if the policy cannot be transferred to a different person and cannot be credit provision; e) electronic money if the value is less than EUR250; f) transactions where the supplier can track the transfer and it is less than EUR1,000; or g) companies whose securities are admitted to public trading on a regulated market in at least one European Union member state or in an equivalent country. However, the institutions always need to take into account the risk of money laundering and terrorist financing. [1]
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence is required in situations that might pose higher money laundering or terrorist financing risk, particularly for: a) transnational relations with institutions acting as correspondents based in countries other than EU or equivalent; b) PEPs; or c) the establishment of a non-face-to-face business relationship.

	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	The Act on counteracting money laundering and terrorism financing 16 Nov 2000 highlights that PEP status applies only to PEPs domicile outside the territory of the Republic of Poland. Article 9e requires that in the case of PEPs obligated institution: a) apply measures, adequate to the risk determined by the institution, in order to establish the source of funds; b) maintain constant monitoring of conducted transactions; c) conclude a contract with a client after having obtained the consent of the board, the designated member of the management board or a person designated by the board or a person responsible for the activities of the obligated institution; and d) may collect written statements on whether a client is a person holding a politically exposed position, which are given under the penal liability for providing data incompatible with the facts. [1]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Article 9e of the Act requires that enhanced due diligence should involve further consideration of the following elements, designed to ensure that the bank has secured a greater level of understanding with corresponding banks overseas (other than those based in the EU or other states with equivalent AML regulations): a) collect information allowing the correspondent to determine the scope of operations and whether the respondent is supervised by a competent regulator; b) assess measures taken by the respondent in counteracting money laundering / terrorism financing; c) prepare documentation determining the scope of responsibilities of the correspondent and respondent; d) ascertain with respect to payable through accounts that the respondent has taken appropriate actions in accordance with procedures on the application of CDD measures in respect of clients having direct access to the respondent's bank accounts and that such information could be provided upon request; and e) obtain consent of senior management. [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Article 9e of the Act requires that establishment of a non-face-to-face business relationships require enhanced due diligence. As a minimum, one of the following actions is required: a) verification of the customer's identity against additional documents; b) certification of copies of identification documents by an appropriate authority; or c) confirmation that the customer's initial transaction was made through an account in the customer's name with another financial institution.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Yes, Article 8 requires that certain transactions above the threshold of EUR15,000 as well as related transactions where the aggregated amount exceeds the threshold should be registered. In case of casino obligation involves any purchase or sale of gambling chips of the value equivalent to at least EUR1,000. [1]

		Article 8 provides exemptions to the requirement to report inter alia in the case of incoming transfers unless they are cross border, or transfers between accounts of the same customer, transfers on the interbank market. In addition, according to Article 8 any obligated institution is required to register a transaction, the circumstances of which may suggest that it was related to money laundering or terrorist financing, regardless of its value and character.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes, Poland has established personal data protection laws. a) yes; b) although corporate data is not considered as personal data, the processing of natural persons' data (such as the representatives of a company) is subject to personal data protection law; and c) Polish data protection law provides a catalogue of "sensitive personal data". They include data on: racial or ethnic origin, political opinions, religious or philosophic beliefs, religion, party or trade-union membership, data concerning health, genetic code, addictions, sexual life, data relating to convictions, decisions on penalty, fines and other decisions issued in any court or administrative proceedings. The processing of such data, as a general rule, is prohibited, unless one of the requirements permitting such processing is provided (e.g. the data subject provides written consent in that respect, such data processing is necessary to protect the data subject's interests, specific provisions of law enable such data processing etc.). Additional protections that apply to the processing of sensitive personal data include: prohibition of processing sensitive personal data before a data filing system is registered in the Polish Data Protection authority's register, an obligation to apply medium security level for protecting the data processed within IT systems without connection to the internet and high security level for protecting the data processed within IT systems connected to the internet. [5] [1]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Polish Personal Data Protection Act, Polish Banking Law and other regulations on professional secrecy (brokerage secrecy, insurance secrecy etc.) including, amongst others, the Act on Financial Instruments Trading, Act on Insurance Activity and Act on Payment Services. Poland does not have a case law in the meaning of institution of common law. However, the jurisprudence of Polish courts and the decisions of the Polish Data Protection authority provide guidelines how to transfer such information.

PORTUGAL		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	N/A
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, Article 7 of Law No.25/2008 provides an exemption for occasional transactions under EUR15,000. For financial institutions, according to Notice 5/2013 of Banco de Portugal, the threshold is EUR15,000 in the case of one off or linked transactions and EUR10,000 and EUR5,000 for cash deposits respectively made by the client or a third person (when the client is considered as high risk client). [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: should provide a valid document with: Full name, signature, date of birth, nationality, address, profession, work address, tax identification number and photo and politically exposed job/function, purpose. Legal persons: should provide a valid document with the headquarters address, identification number (should be made through the card named Cartão de Identificação de Pessoa Colectiva), shareholder identification for individuals who hold more than 25% of the voting rights and identification of the board of directors. For non-resident entities, equivalent documentation is required. [1]
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	The copies of documentation can be certified by external third parties such as notaries.
	In what circumstances are reduced/simplified due diligence arrangements available?	Articles 11 and 25 provide that except where there are suspicions of money laundering or terrorist financing, simplified due diligence can be adopted in the following situations: a) financial entities shall not be subject to the identification requirement where the customer is a financial entity set up in a European Union Member State or in a third country which imposes equivalent requirements in respect of money laundering and terrorist financing prevention; b) the customer is a listed company whose securities have been admitted to trading in a regulated market in any EU Member State, as well as listed companies in third country markets, which are subject to equivalent reporting obligations; c) the customer is the State, autonomous regions, local authorities, a legal person governed by public law, of any nature, integrated in the central, regional or local governments; d) the customer is a public authority or body with transparent accounting practices and subject to monitoring; e) the customer is the entity providing postal services or is the Treasury and Government Debt Agency;

		f) issuance of electronic money, whose monetary value is stored on an electronic device and represents a claim on the issuer, issued on receipt of funds or an amount not less than the monetary value issued and accepted as a means of payment by undertakings other than the issuer; g) life insurance policies, pension fund contracts or similar savings schemes where the annual premium or contribution is no more than EUR1,000 or the single premium is no more than EUR2,500; h) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; and i) pension superannuation or similar schemes that provide retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme. [1]
	In what circumstances are enhanced customer due diligence measures required?	Article 12 provides that entities should apply enhanced due diligence measures in respect of customers and transactions which by their nature or characteristics present a higher risk of money laundering or terrorist financing. This includes: a) non-face-to-face transactions and in particular to those operations that may favour anonymity; b) operations carried out with PEPs resident outside the jurisdiction; and c) correspondent banking operations with credit institutions established in third countries and any others designated by the competent supervisory or monitoring authorities.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Article 12(4) provides that a non-resident PEP relationship requires additional due diligence. When establishing a relationship with some non-resident PEP entities should: a) have appropriate risk-based procedures to determine whether the customer is a PEP; b) have senior management approval for establishing business relationships with such customers; c) take adequate measures to establish the source of wealth and the source of funds that are involved in the business relationship or occasional transaction; and d) conduct enhanced ongoing monitoring of the business relationship.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Enhanced due diligence is not required in the case of correspondent banking relationships with financial institutions in EU Member States. Article 26 provides in the case of cross border relationships with institutions in third countries that the following enhanced due diligence measures should be adopted: a) the correspondent should gather sufficient information about a respondent institution to fully understand the nature of the respondent's business, to assess the respondent institution's anti-money laundering and anti-terrorism financing controls and to determine from publicly available information the reputation of the institution and the characteristics of its supervision; b) approval should be obtained from senior management before the establishment of a new banking relationship and the respective responsibilities documented; and

		c) if the correspondent relationship involves payable through accounts, the institution shall be satisfied that the respondent has verified the identity of the customer and performed due diligence on the customer having direct access to the accounts, ensuring that all these elements of information can be provided upon request. [1]
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Article 12 provides that non face-to-face relationships (especially those that can favour anonymity) require enhanced due diligence. In these cases, the institution should demand additional documentation or information considered adequate to check or certify the data provided by the customer and ensure the first credit or debit is made through an account opened in the customer's name.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	No.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Notice of Banco de Portugal No 9/2012 defines the risk management information report regarding anti-money laundering and terrorism financing internal control. This report must be attached with a formal opinion from the bank's audit committee or equivalent body.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	a) yes; b) notice 25/2008 does not prevent financial institutions and non-financial entities exchanging information that concerns a joint business relationship on the same client, if their sole purpose is preventing money laundering and terrorist financing. In addition, all entities are subject to equivalent obligations of professional secrecy and protection of personal data is established in other Member States of the European Union or equivalent third country prevention of money laundering and terrorist financing; and c) yes.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	No.

ROMANIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	The National Office for Prevention and Control of Money Laundering organises training seminars at least once a year regarding the prevention of money laundering and of financing of terrorist acts. In addition, the National Office for Prevention and Control of Money Laundering has issued a number of guides and handbooks (http://www.onpcsb.ro/html/instruire.php?section=3). [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, transactions below EUR15,000. However, the KYC procedure must be performed for all clients where a transaction appears suspicious and a report should be made to the National Office for Prevention and Control of Money Laundering even if the transaction is lower than EUR15,000. Exceptions: a) casino chip exchange below EUR2,000; and b) life insurance, where the premium or yearly payment of these are lower or equal to the equivalent in of EUR1,000. [1]
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals need to provide the following details: a) name and surname; b) date and place of birth; c) personal identity number or, if is the case, another similar unique element for identification; d) the domicile and, if is the case, the residence; e) telephone number, fax, electronical address, if is the case; f) citizenship; g) qualification as resident or non-resident; and h) the public function, for foreigners that are residents of another country, if is the case. Part of the details above can be verified by an identity card or passport. Legal entities need to provide the following details: a) number, series and the date of the certificate/document of registration with the National Office of Trade Registry or other authorities; b) name; c) unique registration code, or its equivalent for foreign legal entities; d) credit institution and the International Bank Account Number (“IBAN”); e) the complete address of headquarters or, if is the case, of the subsidiary; f) telephone, fax and, if is the case, the email and the internet page; and

		g) the scope and nature of the transactions/operations performed with the customer. Part of the information can be verified by an official extract from The National Trade Registry Office which proves existence of the entity. This applies to customers and beneficiaries as well.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	There are no special requirements, but the verification via independent sources is required for specific clients based on the risk assessment.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence arrangements apply to: a) domestic public authorities; b) life insurance under the conditions mentioned in the law and subscription to pension funds; c) electronic currency as defined by the regulations; d) a credit or financial institution from an European Union ("EU") member state or from the European Economic Area ("EEA"), or a credit or financial institution from a non-EU state or from a state outside the EEA that imposes similar anti-money laundering and counter terrorist financing requirements and supervision; e) entities admitted to trading on EU-based regulated markets or non-EU regulated markets that ensure a similar level of protection; f) beneficial owners from transactions that are performed through collective accounts managed by public notaries, lawyers or similar officers from EU Member States or non-EU states that ensure a similar level of protection; and g) transactions and products that are low risk in respect of money laundering and the financing of terrorist acts.
	In what circumstances are enhanced customer due diligence measures required?	Enhanced due diligence measures are required in the following cases: a) non face-to-face transactions; b) in the case of correspondent relationships with credit granting institutions from non-EU countries and those countries that are not part of the EEA; c) transactions or business relationships with politically exposed persons who are resident in another EU member state or in the EEA, or in non-EU countries or countries outside the EEA; and d) in any other cases where it is considered that due to their nature, a high risk in respect of money laundering and the financing of terrorist acts is present.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Additional due diligence is required for transactions or business relationships with PEPs who are resident in another EU member state or in the EEA, or in non-EU countries or countries outside the EEA.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Enhanced due diligence must be performed for cross-border correspondent banking relationships with credit institutions in third countries.

	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Additional due diligence is required for all non-face-to-face transactions.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Yes, cash transactions in excess of EUR15,000 have to be reported to National Office for Prevention and Control of Money Laundering by individuals and other legal entities that sell goods and services.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	There is no specific legal requirement for an external auditor/other external organisation to report on the bank's AML systems and controls.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes, Romania's personal data protection legislation exists mainly in Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data. a) yes; b) they only apply in relation to the personal data of individuals; and c) yes, it refers to "special categories of data", and it includes personal data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of a similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life, personal data regarding criminal or minor offences, as well as personal identification numbers or of other personal data with a general identification function. Additional protection depends on the category of data. In general, the additional protection consists of the requirement to process such data based exclusively on the express and unequivocal consent of the person. However, the processing of data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life is prohibited or it is very strictly regulated. Processing personal data regarding criminal offences committed by the data subject, or regarding previous criminal convictions, security measures or administrative or minor offence sanctions applied to the data subject, may be carried out only under the control of public authorities, within the limits of their powers given by law and under the terms established by the specific provisions in this field of law.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Any processing of personal data in Romania falls under the protection of the Romanian laws regarding personal data processing.

SLOVAKIA		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes, guidelines for submitting AML notifications issued by the FAU: http://www.minv.sk/?financna-policia AML Guidelines for the financial sector, issued by the National Bank of Slovakia: http://www.nbs.sk/en/financial-market-supervision/prevention-of-legalisation-of-proceeds-of-criminal-activity-and-financing-of-terrorism/recommendations-and-methodical-guidance [5] [1]
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, any single transaction below EUR15,000 does not require any customer due diligence unless it is: a) a suspicious transaction; b) an agreement to enter into a business relationship; c) a transaction with a PEP; d) as part of the business relationship when there are doubts about the veracity or completeness of client's identification data previously obtained; or e) a transaction concerning withdrawal of a cancelled final balance of bearer deposit. Also in the case of life insurance, customer due diligence is not required if the insurance premium payable per year does not exceed EUR1,000, or if payable in a lump-sum, does not exceed EUR2,500, as well as in certain situations related to pension scheme agreements (no amount set by law). An ordinary transaction below EUR2,000 does not need customer due diligence.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: Name, surname, birth identification number or date of birth, place of birth, gender, address and citizenship. These would normally be verified by an identity card or passport. Individuals who conduct business: In addition to the above, full name of the business, place of business and identification number needs to be noted. Legal entities: the full name, residency/seat, identification (or similar identification received from foreign offices) showing evidence of the company's existence (i.e. certificate of incorporation, trade register statement or other). The same principles for 'individuals' apply for the identification of individuals in the company's statutory body. If the company's statutory body or the owner is another legal entity, identification documentation must also be collected for that entity. The way of acting of the statutory representatives, acting on behalf of the legal entity must be proven, e.g. visible from the certificate of incorporation, trade register statement or other similar document, or power of attorney must be provided by the client.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	These should be certified by an appropriate person e.g. a notary, local authorities etc. Specific rules apply to credit and financial institutions, where certain employees are authorised to verify these when opening an account, concluding a contract etc.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence is applicable in the following situations: a) the client is a credit or financial institution within the EU or EEA; b) the client is a listed entity in the EU or EEA; c) the client is public authority (specific conditions detailed in the law); d) the client is Slovak public authority; e) the client is a credit institution or a financial institution which operates in the territory of a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by the Slovak AML Act and with regard to performance of those duties they are supervised;

		f) to the extent of identification and verification of identification of the beneficial owner if a pooled account is managed by a notary or an advocate who operates in the EU or EEA or in a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by this Act and if the data on identification of the beneficial owner are available, on request, to the obliged entity that keeps this account; g) the client is a legal entity with securities negotiable on a regulated market in a EU or EEA or is a company which operates in the territory of a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by Slovak laws. In case of a life insurance contract to be concluded if the insurance premium payable per year does not exceed EUR1,000 or if payable in lump-sum does not exceed EUR2,500; and h) in certain situations related to pension scheme agreements, both mandatory and voluntary (no amount set by law).
	In what circumstances are enhanced customer due diligence measures required?	Enhanced customer due diligence is applicable for: a) a remote financial services agreement; b) a transaction and business relationship with a PEP; and c) a correspondent bank relationship with a foreign credit or similar institution (“correspondent institution”).
	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?	All transactions with PEPs are subject to due diligence including the provision of information and supporting documentation relating to: a) the purpose and intended nature of the transactions or business relationship; b) the beneficial owner, if the client is a legal entity; c) the information required for continuous monitoring of the business relationship; and d) a review of the income source.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Prior to the creation of a correspondent banking relationship, the following is required: a) sufficient information on the relevant correspondent institution and the nature of its operations; b) publicly sourced information to establish the quality of supervision overseeing the correspondent institution; c) an evaluation of measures applied by the correspondent institution against the legitimisation of proceeds of crime and financing terrorism; d) understanding if approval of relevant lead employee to open the corresponding bank relationship was granted; and e) in the case of wire transfers, confirmation from the correspondent bank that it has identified the account holder.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	In the case of a remote financial services agreement: a) the first payment under this agreement shall be made via an account kept in the customer's name held at a credit institution or a foreign credit institution operating in the EU or EEA; and/or

		b) the customer shall submit to the entity a copy of a document verifying the existence of this account together with copies of the relevant parts of his identity card and at least one more identification document to validate the customer's identification data of this card i.e. the type, serial number, issuing country or institution and validity.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Suspicious transactions are identified based on various criteria such as unusual transactions, cash transactions above a certain threshold, international wire transfers etc. but no special report is required.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No. However, if the external auditor during performance of the regular audit procedures finds out facts which indicate a suspicion of committing economic crime, crime against property or crime of corruption, he is obliged to inform the FAU, statutory representatives and control body of the given bank thereof. Internal audit/control body of the bank is the body primarily responsible for AML procedures within the bank.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes. Slovak Act No. 122/2013 Coll. ("the Data Protection Act") governs the area of personal data protection. a) yes; b) the personal data used for corporate purposes are subject to the Data Protection Act. Rules for acquiring, processing, storing, and usage (jointly "processing") of personal data must be complied with in full extent. However, for the purpose of AML, processing of personal data is generally not subject to the consent of affected persons, if their eventual submission to the FAU as a part of SAR is required directly by the law; and c) yes, the Data Protection Act stipulates a separately protected category of personal data. It is forbidden to process personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or political movements, trade union membership and data concerning health or sex life. Personal data regarding mental identity, biometric personal data, and personal data on records of criminal and administrative offences may be processed only by persons designated by relevant laws, and only for specific purposes.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	In general, the AML data provided by the obliged subjects are exempt from any usual restrictions imposed on these types of data. However, each transfer would need to be considered carefully and provided strictly within the extent of the AML law and other applicable legislation, so that no rights or legal entities or natural persons are breached. Generally, transfers of personal data to countries without adequate protection measures (i.e. outside the EEA and EU and Safe Harbour Regime) require approval of the Slovak Personal Data Protection Office. Each case is considered separately.

SPAIN		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	SEPBLAC Reports and Publications: http://www.sepblac.es/espanol/informes_y_publicaciones/otra_documentacion.htm
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes, one-off transactions (single or linked) under EUR1,000.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Individuals: firms should obtain a national identity document, permission of impeachment sent by the Ministry of Justice, passport or government issued document which includes the customer's full name and photograph. Additionally, firms must verify identification documents of all authorised persons of the account. Corporates: firms should obtain the following: full name, regulation form and number, business address and professional activity. Additionally, names and regulation documents of all Attorneys should be obtained.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Copies should be certified by an appropriate person, for example an employee of the commercial office.
	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence could be applied to some concrete clients and products. Detailed requirements for this are detailed in Law 10/2010, Section 2, Articles 9 and 10.
	In what circumstances are enhanced customer due diligence measures required?	The law determines that firms will require additional measures of identification for certain business transactions, including private banking, correspondent banking, online and telephone banking and currency exchanges. Enhanced due diligence must be applied for particular clients and products. Detailed requirements for these activities are detailed in Law 10/2010, Section 3, Article 11: in general terms, and Article 16: for products and transactions where anonymous activity is possible.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Law 10/2010, Articles 14 and 15 detail the due diligence and monitoring requirements for PEPs.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Firms should take into account the greater potential for money laundering in a correspondent business relationship. Firms must send an AML questionnaire to their correspondent banks to verify that these banks have measures to control money laundering. Law 10/2010 Article 13 details the requirements for correspondent banking relationships.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Firms should take account of the greater potential for money laundering in non face-to-face situations. Where a customer approaches a firm remotely (by post, telephone or over the internet), the firm should carry out non face-to-face verification, either electronically, or by reference to identification documents. Requirements for non face-to-face transactions and/or relationships are detailed in Law 10/2010, Article 12.

Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	There are two different types of reporting in Spain: Systematic Reporting and Suspicious Transaction Report.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	Yes, all banks have to be reviewed by an external auditor each year
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes. All the files used by the Entity to manage the AML obligations have to be reported to the Data protection authorities.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	Law 15/1999; Law 2/2011; Law 10/2010; RD 1720/2007; RD 3/2010.

SWEDEN		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Yes: a) by the Swedish Bankers' Association (http://www.penningtvatt.se/); and b) by the financial regulator (http://www.fi.se/Regler/Penningtvatt/).
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	Yes: a) when establishing a customer relationship; b) single transactions at EUR15,000 or more; c) serial transactions together totaling EUR15,000 or more; or d) any transaction, independent of value, if there is suspicion about terrorist financing.

	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Reliable and independent information sources must be used and controls signed off and documented independently whether the customer is a legal or physical entity. For example, evidence of identity can be in document or electronic form. The following information is required: Individuals: approved identification documents with name and social security number. Remote customers can be identified with an approved electronic identity card to verify name, social security number and address. Foreigners must be identified through a passport and a copy must be kept. Legal entities: official registration documents and the identity of representatives through approved identification documents.
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	Third parties can be used or the financial institution can choose to perform these controls in-house. However, the financial institution always has responsibility for identification procedures and ensuring compliance with laws and regulations.
	In what circumstances are reduced/simplified due diligence arrangements available?	a) Swedish public authorities; b) firms within the European Union ("EU") / European Economic Area ("EEA") and specified countries that have similar AML/CFT legislation that conduct business as: a. banks (as defined by Swedish law); b. life insurance companies; c. securities firms (as defined by Swedish law); d. certain other financial firms that are registered with the Swedish Financial Services Agency ("FSA") (as defined by Swedish law); e. insurance brokers (as defined by Swedish law); f. firms that issue electronic money (as defined by Swedish law); g. mutual funds (as defined by Swedish law); and h. registered payment service providers and payment institutions (as defined by Swedish law); c) firms whose shares are listed on an exchange within the EU/EEA as defined by 2004/39/EU or listed on an exchange outside the EU/EEA where the requirements correspond to 2004/39/EU; d) life insurance products with an annual premium of maximum EUR 1,000 or a one off premium of maximum EUR2,500; e) certain occupational pensions; f) electronic money with certain thresholds as defined by Swedish law not exceeding EUR 250; and g) certain pooled accounts in the EU/EEA or in territories outside the EU/EEA provided that certain requirements are met. [1] [4]
	In what circumstances are enhanced customer due diligence measures required?	a) when a business relationship is established or an individual transaction is carried out with another at a distance;

		b) when establishing a business relationship or if executing a single transaction with a PEP; c) correspondent banking relationships with credit institutions outside the EU/EEA; and d) when the risk of money laundering or financing of terrorism is deemed to be high.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	a) at the establishment of a business relationship; and b) for single transactions.
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Gather sufficient information about the bank in order to assess the reputation of the bank and the quality of supervision, assess the bank's AML/CFT controls, document the controls of each institution, obtain internal approval to establish a correspondent banking relationship and verify that the bank undertakes KYC procedures of its customers and can provide relevant information.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	When a business relationship is established or an individual transaction is carried out with another at a distance, such as opening bank accounts online.
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	No.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No, but if there is a lack of control the auditor is obliged to report to the board of directors.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	a) yes; b) the Swedish Personal Data Act only covers information relating to individuals; and c) yes, there are general restrictions in Sweden, but exemptions exist for institutions that are required to report suspicious transactions. These institutions can process the personal data of individuals provided they do not process data other than name, social security/organisation number, address and supporting data/documents constituting reason for suspicion. Restrictions also exist for how and when registers need to be cleansed. The upgrade of the Swedish Act on Combatting money laundering and terrorism on 01 Aug 2015 has introduced possibilities to process sensitive data when identifying PEPs and for the record keeping of such data or data related to the monitoring of PEPs.
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	No.

UK		
Category	**Question**	**Answer**
Regulatory Environment	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.	Key sources of practical guidance with regard to AML requirements include: a) the FCA's Financial Crime Guide for Firms Part 1 (Apr 2015) (https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf) and the FCA's Financial Crime Guide for Firms Part 2 (Apr 2015) (https://www.handbook.fca.org.uk/handbook/document/FC2_FCA_20150427.pdf); b) Joint Money Laundering Steering Group ("JMLSG") Guidance Parts 1 and 2 (http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current); c) Gambling Commission: Money Laundering: the prevention of money laundering and combating the financing of terrorism – Guidance for remote and non-remote casinos, second edition (July 2013) (http://www.gamblingcommission.gov.uk/pdf/prevention%20of%20money%20laundering%20and%20combating%20the%20financing%20of%20terrorism%20-%20july%202013.pdf); d) ICAEW (http://www.icaew.com/en/technical/legal-and-regulatory/money-laundering/uk-law-and-guidance); e) HMRC (http://www.hmrc.gov.uk/MLR/); and f) The Law Society (http://www.lawsociety.org.uk/support-services/risk-compliance/anti-money-laundering/).
Customer Due Diligence	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?	No.
	What are the high level requirements for verification of customer identification information (individuals and legal entities)?	Evidence of identity can be in documentary or electronic form. Individuals: full name, residential address and date of birth ideally from a government issued document which includes the customer's full name and photo, and either residential address or date of birth e.g. valid passport, valid photo card driving licence etc.; or a government issued document (without a photograph) which includes the customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FCA-regulated firm in the UK financial services sector or in an equivalent jurisdiction, which includes the customer's full name and either residential address or date of birth. Corporates (other than regulated firms): full name, registration number, registered office in country of incorporation and business address. Additionally, for private / unlisted companies: names of all directors (or equivalent), names of individuals who own or control over 25% of its shares or voting rights and names of any individual(s) who otherwise exercise control over the management of the company. The firm should verify the existence of the corporate from either confirming the company's listing on a regulated market, conducting a search of the relevant company registry or obtaining a copy of the company's Certificate of Incorporation. For private / unlisted companies, the firm may decide, following a risk assessment, to verify one or more of the directors as appropriate in line with the CDD requirements for individuals. In respect of beneficial owners, the relevant person must take risk based and adequate measures to verify the identity of the beneficial owner(s).
	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?	UK AML Guidance states that where identity is verified electronically, or copy documents are used, the firm should apply an additional verification check to manage the risk of impersonation fraud. For example, one of these checks may be to require copy documents to be certified by an appropriate person.

	In what circumstances are reduced/simplified due diligence arrangements available?	Simplified due diligence may be applied to: a) certain regulated firms in the financial sector; b) companies listed on a regulated market subject to specified disclosure obligations; c) beneficial owners of pooled accounts held by notaries or independent legal professionals; d) UK public authorities; e) European Community institutions; f) certain life assurance and e-Money products; g) certain pension funds; h) certain low risk products; and i) child trust funds and junior ISAs.
	In what circumstances are enhanced customer due diligence measures required?	A firm must apply, on a risk-sensitive basis, enhanced customer due diligence measures and enhanced ongoing monitoring in any situation which by its nature can present a higher risk of money laundering or terrorist financing. The three specific types of relationship in respect of which enhanced due diligence measures must be applied are: a) where the customer has not been physically present for identification purposes; b) in respect of a correspondent banking relationship with Respondents from non-European Economic Area ("EEA") states; or c) in respect of a business relationship or an occasional transaction with a PEP.
	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?	Where a firm proposes to establish a business relationship or carry out a one off transaction with a PEP the relevant person must: a) have appropriate risk based procedures to determine whether a customer is a PEP; b) obtain appropriate senior management approval for establishing the business relationship with that customer; c) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and d) conduct enhanced ongoing monitoring of the relationship. [11]
	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?	Enhanced customer due diligence must be undertaken by Correspondents on Respondents using a risk based approach. The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken: a) the Respondent's domicile; b) the Respondent's ownership and management structures;

		c) the Respondent's business and customer base; and d) downstream Correspondent Clearing. Where a Correspondent bank is outside the EEA, the UK bank should thoroughly understand its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must give approval to each new correspondent banking relationship.
	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?	Where a customer has not been physically present for identification purposes, a firm must take specific and adequate measures to compensate for this higher risk by applying one or more of the following measures: a) ensuring that the customer's identity is established by additional documents, data or information; b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the Money Laundering Directive; or c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution. [11]
Reporting	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	Where firms believe that they hold funds or assets for a sanctioned party, this must always be reported to the Asset Freezing Unit at HM Treasury as soon as practicable. There are no other specific reporting obligations outside of suspicious transactions.
AML Audits	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?	No.
Data Privacy	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?	Yes. The processing or retaining of personal data in the UK is governed by the Data Protection Act 1998 (DPA): a) the DPA regulates the processing of 'personal data'. The information obtained/retained by a relevant person for the purposes of customer due diligence would fall within the definition of personal data; b) the DPA only applies to individuals and not legal persons. It therefore does not extend protection to corporate data; and c) yes. Section 2 of the DPA provides a separate definition of "sensitive personal data" which relates to personal data consisting of information as to the racial or ethnic origin of the data subject, their political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, their sexual life, their commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. In addition to meeting one of the conditions for processing in Schedule 2 of the DPA, at least one of several other conditions listed in Schedule 3 of the DPA must be met in the case of processing of sensitive personal data. Additional regulations such as the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders also provide that sensitive

		personal data can be processed where there is substantial public interest, such as the prevention or detection of crime, and protecting the public against malpractice or maladministration. For further information, see 'The Guide to Data Protection' published by the Information Commissioner's Office: http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf [1] [4] [2]
	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?	The DPA regulates the sending of personal data outside of the EEA. The Act contains a prohibition on data being sent to countries that do not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. No corresponding provisions exist governing the receipt of personal data from countries outside the EEA. Once received by an entity or individual within the United Kingdom, the data is subject to the requirements of the DPA.

6.1.2 Summary evaluation of VIMPay in relation to the EU regulatory requirements

The current fundamental regulatory requirements for a global European market entry as described in the individual European country tables above favor VIMpay. The core of the EU regulatory requirements has been addressed and factored into the VIMpay AML and customer due diligence infractucture as part of the VIMpay KYC models.

1. Regulatory Environment

For the EU SEPA region there is practical guidance provided by public authorities regarding AML requirements beyond the FATF recommendations. No additional adjustments to the VIMpay regulatory infrastructure are required since all the requirements are satisfied.

2. Customer Due Diligence

The VIMpay Freemium monetization strategy falls in line with global EU customer due diligence requirements. The VIMpay Premium version has transaction threshholds that fit in with the EU threshholds in place. The KYC models utilized for VIMpay fall within the KYC parameter for the individual EU country requirements to support a Pan-European market entry.

3. Reporting

As an addition to the customer due diligence, the reporting obligations for transactions over the set threshholds in each EU country have been factored into the VIMpay AML and customer due diligence strategy. Therefore, there is no need for a change in the VIMpay reporting culturte.

4. AML Audits

As part of the reporting regime that is currently implemented into the VIMpay AML and customer due diligence infrastructure, all out-of-threshhold transactions will be reported. This will automatically satisfy AML audit requirements in all the applicable EU countires.

5. Data Privacy

Within the VIMpay KYC models, there are no touch points where data privacy infrigements might occur as defined and elaborated by the EU data protection laws and the individual EU country amendments

7 Conclusion

The market conditions are extremely favorable for the adoption of VIMpay in Europe. The current European demographics support the VIMpay business case with very minimal and non-project-threatening technical adjustments.

With the adoption of PSD II, VIMpay is set to greatly benefit. PSD II effectively removes the previously mentioned potential challenge in offering the VIMpay with multi-banking capabilities in Europe.

Existing regulatory and legal requirements in Europe fall mostly in line with the current VIMpay infrastructure. There are built-in VIMpay protocols and processes to satisfy the existing European AML / CFT requirements. Where there are slight discrepancies, practical guidance is provided by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation.

VIMpay customer due diligence protocols will satisfy European customer due diligence and reporting requirements. The stringent European data protection policies and guidelines are adhered to in VIMpay. This falls in line with the individual European country requirements.

References on the EU Market Research

[1] PWC, "KYC Quick Reference Guide," January 2016.

[2] http://www.knowyourcountry.com/, "KnowYourCountry.com," 2016.

[3] C. o. Europe, "FATF Report Money Laundering through Money Remittance and Currency Exchange Providers," June 2010.

[4] http://kycmap.com/about/, "kycmap.com," 2016.

[5] E. &. Young, "Anti-money laundering and sactions investigations," 2014.

[6] http://ec.europa.eu/, "http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm," 2016.

[7] C. o. Europe, "Third Round Detailed Assessment Report on Bulgaria - Anti-Money Laundering and Combating The Financing of Terrorism: MONEYVAL (2008) 02," Strasbourg, April 2008.

[8] U. D. o. Treasury, "Agreement between the Government of the United States of America and the Government of the Republic of Bulgaria to Improve International Tax Compliance and to Implement FATCA," February 2007.

[9] http://www.knowyourcountry.com/, "Bulgaria Risk & Compliance Report January 2016," January 2016 .

[10] I. M. Fund, "Republic of Lithuania Article IV Consultation - Staff Report; Press Release; And Statement by the Executive Director for the Republic of Lithuania," 2014.

[11] https://www.seb.lt/eng/about-seb/about-seb/other/anti-money-laundering-policy, "Anti Money Laundering Policy".