

GUIDELINES ON THE IMPLEMENTATION OF THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING ACT (ZPPDFT-2)

adopted at the session of the Bar of Lawyers of the Bar Association of Slovenia on 19 April 2023

Note: These Guidelines are advisory in nature and intended to support lawyers and law firms in the implementation and understanding of the provisions of the ZPPDFT-2.

1. INTRODUCTION

On 19 November 2016, the Prevention of Money Laundering and Terrorist Financing Act (ZPPDFT-1) entered into force. It transposes into Slovenian legislation the fourth European Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.

On 22 November 2022, the Prevention of Money Laundering and Terrorist Financing Act (ZPPDFT-2) entered into force. The purpose of the new Act is to transpose the provisions of the aforementioned Directive into the Slovenian legal system, to comply with the international recommendations. The ZPPDFT-2 introduces a number of improvements that do not affect the concept of the previous ZPPDFT-1 or its fundamental provisions. Instead, by eliminating certain inconsistencies and ambiguities, easing certain requirements and introducing additional tools and options for the implementation of measures by obliged entities and schemes for supervising the Act's implementation, it ensures the more effective management of the risk of money laundering and terrorist financing by obliged entities and the implementation of supervision.

The proposed Act also transposes part of the provisions of Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122; hereinafter: Directive (EU) 2019/1153) and Directive (EU) 2019/2177 of the European Parliament and the Council amending Directive 2009/138/EC on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Directive (EU) 2014/65 on markets in financial instruments and Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing (Text with EEA relevance) (OJ L 334, 27.12.2019, No 155; hereinafter: Directive (EU) 2019/2177) and regulated in more detail the implementation of Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (OJ L 284 of 12.11.2018, p. 6; hereinafter: Regulation (EU) 2018/1672).

The ZPPDFT-2 authorises the Bar Association of Slovenia, in its capacity as the primary supervisory body of lawyers and law firms, to issue recommendations and guidelines relating to the implementation of the measures prescribed for the detection and prevention of money laundering and terrorist financing.

The obliged entities under the ZPPDFT-2 must produce a risk assessment within 18 months of issuing the Guidelines; within 2 years of the entry into force of the ZPPDFT-1, for existing customers, establish their beneficial owner and whether the existing parties, their legal representatives, authorised persons or beneficial owners are politically exposed persons (the obligation to identify such exposure applies

only to those customers, legal representatives, authorised persons or beneficial owners for whom, prior to the entry into force of the ZPPDFT-1, there was no obligation to determine whether they were politically exposed persons).

2. SUBJECT OF THE ZPPDFT-2

The Act introduces a risk-based approach at the national and supranational levels, at the level of obliged entities and within the operational scope of supervisory institutions.

The obligation to carry out customer due diligence as one of the essential anti-money laundering and terrorist financing measures is extended to those cases where occasional transactions involve transfers of funds exceeding EUR 1,000. The limit above which obliged entities are required to report cash transactions to the Office is EUR 15,000.

One of the major new elements of the ZPPDFT-1 and ZPPDFT-2 is the introduction of the Beneficial Owners Register. Business entities registered in the Slovenian Business Register will be required to identify their beneficial owners and enter the relevant data in the Beneficial Owners Register, which will be maintained and managed by the Agency of the Republic of Slovenia for Public Legal Records and Related Services (AJPES). Another purpose of the Register is to provide obliged entities with access to relevant data for the purposes of carrying out customer due diligence.

A key change relates to politically exposed persons, since the term "foreign politically exposed person" is replaced by the term "politically exposed person", meaning any natural person who is or was entrusted with a prominent public function within the previous year in a Member State or in a third country. This means that the obligation of enhanced customer due diligence will now apply not only to foreign persons but also to "domestic" politically exposed persons acting in a prominent public function in the Republic of Slovenia.

Under the new arrangement, the Office for Money Laundering Prevention is also granted powers to carry out inspections. This will enable it to carry out inspections of obliged entities that do not have a primary supervisor and, if necessary, to carry out inspections of other obliged entities who already have a primary supervisor (i.e. lawyers and law firms; in this respect, the ZPPDFT-2 incorporates safeguards similar to those included in law enforcement investigations of law firms). The Act also provides for cooperation and carrying out supervision together with other primary supervisors. With regard to lawyers, the ZPPDFT-2 contains specific provisions concerning the exercise of supervision by the Office. Safeguards are introduced into the Act to protect the principle of lawyer–customer confidentiality.

With regard to criminal provisions, the Act introduces stricter sanctions in accordance with Directive (EU) 2015/849 for those offences deemed particularly serious due to the amount of damage caused, the amount of illegal proceeds, the intent of the perpetrator, their intention to take advantage, and the repetition or systematic nature of the offence.

3. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering means any handling of money or property derived from a criminal offence, including:

1. The conversion or transfer of money or other proceeds of crime;
2. The concealment or disguise of the true nature, origin, location, movement, disposition, ownership or rights in respect of money or other property derived from a criminal offence.

Terrorist financing means the provision, collection, or attempted provision or collection of money or other property, whether of legal or illegal origin, directly or indirectly, with the intent or knowledge that it will be used, in whole or in part, to commit an act of terrorism or any other act related to terrorism, or that it will be used by a terrorist or a terrorist organisation.

4. TASKS OF LAWYERS AND LAW FIRMS UNDER THE NEW ZPPDFT-2 (Articles 17 and 90 of the ZPPDFT-2)

Lawyers and law firms become obliged entities under the ZPPDFT-2 and are obliged to implement measures to detect and prevent money laundering and terrorist financing and to apply these Guidelines only in the case referred to in Article 90 of the ZPPDFT-2, namely when:

1. Assisting in planning or executing transactions for a customer concerning:
 - a) Buying or selling real property or a company;
 - b) Managing a customer's money, securities or other property;
 - c) Opening or managing bank, savings or securities accounts;
 - č) Raising the funds required to establish, operate or manage a company;
 - d) Establishing, operating or managing foundations, trusts, companies or other similar legal organisational forms;
2. Carrying out a financial or real estate transaction on behalf of and for a customer.

Lawyers, law firms or notaries must report all cases in which a customer seeks advice for the purpose of money laundering or terrorist financing to the Bar Association of Slovenia immediately or no later than within three business days of the date the advice was sought.

Tasks of lawyers and law firms when they are obliged entities under Article 90 of the ZPPDFT-2:

1. Making a risk assessment of money laundering and terrorist financing (within 18 months of issuing the Guidelines), regular updating;
2. Establishment, implementation and monitoring of the implementation of policies, controls and procedures to manage money laundering and terrorist financing risks, and monitoring compliance with the requirements stipulated by regulations;
3. Implementing measures to acquire knowledge about the customer (hereinafter: customer due diligence) under the terms and conditions and in the manner provided by this Act;
4. Reporting of data to the Office of the Republic of Slovenia for Money Laundering Prevention (Note: new reporting form in use);
5. Appointing an AML/CFT Compliance Officer and their deputies and ensure conditions for their work;
6. Provision of regular professional training and education for employees;
7. Preparation of a list of indicators for identifying customers and transactions where there are grounds to suspect money laundering or terrorist financing;

- | |
|--|
| <ol style="list-style-type: none">8. Ensuring <u>data protection and retention</u> and management of <u>records</u> pursuant to the ZPPDFT-1;9. Implementation of group policies and procedures and measures to detect and prevent money laundering and terrorist financing in own branches and majority-owned subsidiaries in third countries;10. Performing other tasks and duties under the ZPPDFT-1 and the regulations issued thereunder. |
|--|

Obligated entities may perform one or more tasks referred to in Article 90 of the ZPPDFT-2 with the assistance of one or more contractors, except the tasks referred to in points 4, 5, 6, and 9 of the preceding paragraph. If the obliged entity is part of a group, one or more tasks referred to in the preceding paragraph, except for the appointment and performance of the tasks of the AML/CFT Compliance Officer referred to in Article 83 of this Act, may be performed with the assistance of a contractor who is part of the same group, provided that the requirements of Article 135 have been met.

In addition to the above, lawyers and law firms that are obliged entities under the ZPPDFT-2 must, within 2 years of the entry into force of the Act (i.e. by 19 November 2018), determine whether the existing customers, their legal representatives, authorised persons and beneficial owners are politically exposed persons (this obligation applies only to those customers, legal representatives, authorised persons and beneficial owners for whom, prior to the entry into force of the ZPPDFT-1, there was no obligation to determine whether they were politically exposed persons).

Lawyers and law firms must report all cases in which the customer seeks advice for money laundering or terrorist financing purposes to the Bar Association of Slovenia immediately or no later than within three business days of the date the advice was sought. Lawyers and law firms must decline to provide further advice. If there are reasonable grounds to suspect money laundering or terrorist financing, the Bar Association of Slovenia must inform the Office immediately, or no later than three working days after receiving a report from the lawyer or law firm.

4.1 RISK ASSESSMENT (Article 18 of the ZPPDFT-2)

The risk of money laundering or terrorist financing means the risk that a customer would misuse the financial system to launder money or for terrorist financing or that a business relationship, transaction, product, service or distribution channel, taking into account the geographical factor (country or geographical area), would be used, directly or indirectly, for money laundering or terrorist financing. A risk analysis is a procedure in which lawyers and law firms define criteria that enable the classification of each customer as a high or low risk customer with regard to money laundering or terrorist financing; it also determines the measures to manage these risks effectively.

A risk analysis is a procedure in which lawyers and law firms define criteria that enable the classification of each customer as a high or low risk customer with regard to money laundering or terrorist financing; it also determines the measures to manage these risks effectively.

A written risk assessment for money laundering and terrorist financing prevention (Article 18 in conjunction with Article 192 of the ZPPDFT-2) must be produced within 18 months of the entry into force of the ZPPDFT-2. The written risk assessment must be approved by the management of the law firm.

The risk assessment must be structured across three levels as follows:

1. At group level (taking into account geographical risk factors for potential abuse):
 - ☐ Particular group or type of customer;
 - ☐ Business relationship;
 - ☐ Transaction;
 - ☐ Product;
 - ☐ Service;
 - ☐ Distribution channel.
2. Based on the risks identified above, the obliged entity assesses the risk of its operations (obliged entity risk assessment).
3. Based on the risks identified above (by group, customer, etc. and obliged entity risk assessment), the obliged entity makes an assessment of each customer (customer risk assessment).

The risk assessment form prepared by the Bar Association of Slovenia (for assessing the risk associated with customers and transactions) may be used as a tool in preparing the risk assessment.

The produced risk assessment must reflect the specific characteristics of a law firm's operations.

The questions to be considered when carrying out a risk assessment include, but are not limited to, the following:

- ☐ Do you have a high turnover and a stable customer base?
- ☐ Do you have customers established in jurisdictions where there is a higher risk of money laundering or terrorist financing?
- ☐ Do you have customers operating in sectors which, by their very nature, pose a higher risk of money laundering or terrorism financing?
- ☐ Whether and how often you work for politically exposed persons (Article 66 of the ZPPDFT-2). Politically exposed persons are now considered to be both domestic and foreign politically exposed persons. Obligated entities must therefore establish an appropriate risk management system that includes a procedure for determining whether a customer, its legal representative or authorised person is a politically exposed person as defined in Article 61 of the ZPPDFT-1. The obliged entities may choose the method for identifying which customers have the status of politically exposed persons, such as survey questionnaires, publicly accessible data, data from the media, the internet, commercial databases and similar. Obligated entities must define this method in their internal acts, taking into account the risk assessment under Article 18 of the ZPPDFT-2 and these Guidelines. Further information on politically exposed persons is available on the Office's website:
http://www.uppd.gov.si/si/opozorila_in_mnenja_urada/mnenja/politico_izpostavljene_osebe/
- ☐ Whether and how often do you work for customers without meeting them personally. What are the areas of law that you cover?

Various sources addressing the implementation of a risk-based approach (e.g. FATF recommendations) show that, when assessing risk, the following criteria are usually taken into account:

- ☐ Customer risk: this includes the risks represented by a customer's status and/or activity (e.g. a politically exposed person, government authority, a customer whose activity is linked to cash operations, charity and non-profit organisations, and similar);

- ☐ Geographical area risk: Countries without proper money laundering and terrorist financing prevention systems, countries with high levels of corruption or crime, countries subject to restrictive measures imposed by international organisations;
- ☐ Product risk or service risk: This includes an individual product or service risk with respect to its potential misuse for money laundering or terrorist financing purposes (e.g. electronic transfer of funds).

To conduct a risk assessment, you can also use the Lawyer's Guide to Detecting and Preventing Money Laundering and Terrorist Financing, which was developed in cooperation with the IBA and ABA (CCBE) ([in English](#)).

Based on the findings of the risk assessment, appropriate measures must be taken to mitigate and manage the risk of money laundering or terrorist financing. In addition, the findings of the risk assessment determine the type of customer due diligence to be performed (simplified, normal or enhanced – Article 19 of the ZPPDFT-2). If you assess that a customer, business relationship, transaction, product, service, distribution channel, country or geographical area pose a negligible risk of money laundering or terrorist financing, conduct simplified customer due diligence (Articles 62 and 63 of the ZPPDFT-2); if the risk is assessed as increased, conduct enhanced customer due diligence (Articles 64 to 70 of the ZPPDFT-2).

WARNING: It is necessary to update the findings of the risk assessment every two years and whenever a significant change in your business process occurs (examples of relevant changes in the business process are listed in Article 18 of the ZPPDFT-2).

4.2 POLICIES, CONTROLS AND PROCEDURES (Article 20 of the ZPPDFT-2)

Written policies, controls and procedures to effectively manage and mitigate money laundering and terrorist financing risks identified in the risk assessment must be established, implemented and maintained. These must be proportionate to the size of your activity (taking into account your size and organisational structure, the scale and nature of transactions, the types of customers you deal with, and the products you offer). They must be approved by the law firm's management, regularly reviewed and updated, and clearly communicated within the law firm.

Your policies, controls and procedures must include:

1. The development of internal policies, controls and procedures relating to:

- ☐ Risk management models; ☐
- ☐ Customer due diligence; ☐
- ☐ Reporting of data to the Office; ☐
- ☐ Data protection and retention and records management; ☐
- ☐ Internal control of the performance of tasks related to detection and prevention of money laundering and terrorist financing; ☐
- ☐ Ensuring regulatory compliance; ☐
- ☐ Secure recruitment and, where appropriate, security clearance of employees in accordance with the Act governing classified data; ☐

2. The establishment of an independent internal audit department to verify internal policies, controls and procedures referred to in the preceding point if the obliged entity is a medium-sized or large company under the Act governing companies (and the appointment of one of the members of the administrative/management body responsible for performing tasks relating to policies, controls and procedures and for ensuring compliance therewith).

In addition to the above in point 1 (your risk management models, how you perform customer due diligence, etc.), it is recommended that your rules, procedures and controls include:

- ☐ Identification and review of complex and unusually large and unusual patterns of transactions that do not have a clear economic or legal objective and other activities which you believe are likely to be related to money laundering or terrorist financing; ☐
- ☐ Taking additional measures, where appropriate, to prevent money laundering or terrorist financing in respect of products and services favouring anonymity; ☐
- ☐ Taking appropriate measures to assess and, if necessary, mitigate money laundering and terrorist financing risks once new technology is introduced. ☐

Your systems, policies, procedures and controls must be risk-based, which means that you must focus your resources on the areas that pose the greatest threat of money laundering and terrorist financing.

4.3 CUSTOMER DUE DILIGENCE (Article 22 et seq. of the ZPPDFT-1)

Through customer due diligence, you establish and confirm their identity and learn about the purpose of the transaction or the intended nature of the business relationship (to reduce the risk of doing business with an unknown customer who might try to use you for money laundering or terrorist financing).

The obligation to carry out customer due diligence exists:

- ☐ When establishing a business relationship with a customer; ☐
- ☐ When carrying out a transaction amounting to EUR 15,000 or more, whether carried out individually or as part of a series of transactions that are clearly linked; ☐
- ☐ Where there are doubts concerning the veracity and adequacy of previously obtained data about a customer or its beneficial owner; ☐
- ☐ Whenever there are grounds for suspicion of money laundering or terrorist financing in respect of a transaction, customer, assets or property, irrespective of the transaction amount. ☐

Lawyers and law firms are not subject to a prohibition on entering into a business relationship (or an order to terminate a business relationship) or on carrying out a transaction if they are unable to take the measures referred to in indents one, two and three below (Subsection 4.3.1) provided they establish the legal position of the customer or if they are representing a customer in legal proceedings (which includes advice on proposing or avoiding such proceedings) – Article 91 of the ZPPDFT-2.

4.3.1 Normal customer due diligence

In general, the obliged entity is required to carry out normal customer due diligence; while at the same time Article 61 of the ZPPDFT-2 envisages two special forms of customer due diligence, i.e. enhanced and simplified customer due diligence.

In accordance with the Act, you must take measures (components of the customer due diligence) as part of normal customer due diligence as follows:

- ☐ Establish the customer's identity and verify their identity on the basis of an independent and reliable source by:
 - a) Inspecting the official identity document of the customer in person, in addition to that of another valid official document; if you doubt the truthfulness of the data obtained or the veracity of the documents submitted, you must request a written statement from the customer (Article 29 of the ZPPDFT-1); if the customer is represented by an authorised person, the authorisation or right to representation is also verified (Articles 30 and 31 of the ZPPDFT-2);
 - b) Verifying the identity of a legal entity by inspecting the original or certified public register documents, which may not be more than three months old and should be submitted by the statutory representative of the legal entity or its authorised person (Article 36 ZPPDFT-2);
- ☐ Identifying the beneficial owner of the customer (A beneficial owner is any natural person who ultimately owns or supervises or otherwise exercises oversight of a customer or a natural person on whose behalf a transaction is carried out; Article 40 of the ZPPDFT-2 et seq.) by inspecting the original or certified documents from a public register, which may not be more than three months old (Article 45 of the ZPPDFT-2); if all the data cannot be obtained from the public register, the missing data is obtained by inspecting the original or certified documents and other business records submitted by the legal representative of the legal person or their authorised person;
- ☐ Obtaining data on the purpose and intended nature of the business relationship or transaction or other data required by law by consulting the original or certified documents and other business documents – for details on the required data, see below (Article 48 in conjunction with Article 137 of the ZPPDFT-1);
- ☐ Regularly and closely monitoring the business activities carried out by the customer through your services (Article 54 of the ZPPDFT-2).

If you are not establishing a customer's legal position or representing a customer in legal proceedings, all of the above measures must still be implemented; however, the extent of their implementation may be adjusted according to the identified risk of money laundering and terrorist financing. In determining the appropriate extent, it is necessary to take into account at least the following:

- ☐ The purpose and nature of the business relationship,
- ☐ The amount of assets, the value of property or the volume of transactions,
- ☐ The duration of the business relationship,
- ☐ Business compliance with the purpose of entering into a business relationship.

The procedures for implementing these measures must be defined in your internal regulations.

WARNING: You must be able to provide supervisory authorities with appropriate documents and data demonstrating that the measures taken are appropriate in view of the risks identified.

What data must be obtained during the customer due diligence (Article 53 of the ZPPDFT-2)?

a) When entering into a business relationship with a customer, lawyers and law firms are required to obtain the following data:

- ☐ Company name, address, registered office, registration number and tax ID number (of a legal entity, sole proprietor or self-employed person entering into a business relationship or carrying out a transaction or on whose behalf a business relationship is established or a transaction carried out);☐
- ☐ Personal name, address of permanent and temporary residences, date and place of birth, tax number or personal identification number (EMŠO), citizenship, and number, type and title of the issuer of the official identity document (of a natural person or their statutory representative, sole proprietor or self-employed person who enters into a business relationship or carries out a transaction; of a statutory representative of a legal person entering into a business relationship or carrying out a transaction; of an authorised person of a natural person, an individual sole proprietor or an individual carrying out an activity on their own, who enters into a business relationship or carries out a transaction; of an authorised person who enters into a business relationship for a legal entity or another civil law entity referred to in point 5 of Article 3 of this Act or carries out a transaction);☐
- ☐ The purpose and intended nature of the business relationship, including information on the activity carried out by the customer;☐
- ☐ The date of entering into the business relationship;☐
- ☐ For beneficial owners: a) personal name, address of permanent and temporary residences, date of birth, citizenship and share of ownership or other means of control; b) in the case referred to in point b) of paragraph one of Article 37 of this Act, information on the category of persons whose interest is the establishment and operation of a foreign trust, foreign institution or similar foreign law legal entity.☐

When carrying out a transaction amounting to EUR 15,000 or more, whether carried out individually or as part of a series of transactions that are clearly linked, lawyers and law firms must, within the scope of customer due diligence, obtain the following data:

- ☐ Company name, address, registered office, registration number and tax ID number (of a legal entity, sole proprietor or self-employed person entering into a business relationship or carrying out a transaction or on whose behalf a business relationship is established or a transaction carried out);☐
- ☐ Personal name, address of permanent and temporary residences, date and place of birth, tax number or personal identification number (EMŠO), citizenship, and number, type and title of the issuer of the official identity document (of a natural person or their statutory representative, sole proprietor or self-employed person who enters into a business relationship or carries out a transaction; of a statutory representative of a legal person entering into a business relationship or carrying out a transaction; of an authorised person of a natural person, an individual sole proprietor or an individual carrying out an activity on their own, who enters

into a business relationship or carries out a transaction; of an authorised person who enters into a business relationship for a legal entity or another civil law entity referred to in point five of Article 3 of the ZPPDFT-2 or carries out a transaction);☐

- ☐ The date and time of the transaction;☐
- ☐ The amount of transaction and currency in which the transaction is carried out;☐
- ☐ The purpose of transaction, personal name, address of permanent and temporary residence, or company name and registered office of the person to whom the transaction is directed, and the country to which the transaction is made;☐
- ☐ The transaction execution method;☐
- ☐ For beneficial owners: a) personal name, address of permanent and temporary residences, date of birth, citizenship and share of ownership or other means of control; b) in the case referred to in point b) of paragraph one of Article 37 of this Act, information on the category of persons whose interest is the establishment and operation of a foreign trust, foreign institution or similar foreign law legal entity.☐

c and ě) in the event of doubt as to the veracity and adequacy of previously obtained data about a customer or beneficial owner and whenever there is a suspicion of money laundering or terrorist financing associated with a transaction, customer, assets or property, irrespective of the transaction amount, lawyers and law firms are required to obtain the following data:

- ☐ Company name, address, registered office, registration number and tax ID number (of a legal entity, sole proprietor or self-employed person entering into a business relationship or carrying out a transaction or on whose behalf a business relationship is established or a transaction carried out);☐
- ☐ Personal name, address of permanent and temporary residences, date and place of birth, tax number or personal identification number (EMŠO), citizenship, and number, type and title of the issuer of the official identity document (of a natural person or their statutory representative, sole proprietor or self-employed person who enters into a business relationship or carries out a transaction; of a statutory representative of a legal person entering into a business relationship or carrying out a transaction; of an authorised person of a natural person, an individual sole proprietor or an individual carrying out an activity on their own, who ☐ enters into a business relationship or carries out a transaction; of an authorised person who enters into a business relationship for a legal entity or another civil law entity referred to in point five of Article 3 of the ZPPDFT-2 or carries out a transaction);☐
- ☐ The purpose and intended nature of the business relationship, including information on the activity carried out by the customer;☐
- ☐ The date of entering into the business relationship;☐
- ☐ The date and time of the transaction;☐
- ☐ The amount of transaction and currency in which the transaction is carried out;☐
- ☐ The purpose of transaction, personal name, address of permanent and temporary residence, or company name and registered office of the person to whom the transaction is directed, and the country to which the transaction is made;☐
- ☐ The transaction execution method;☐

- ☐ Data on the origin of assets and property that is or will be the subject of a business relationship or transaction; ☐
- ☐ Personal name, address of permanent and temporary residences, date and place of birth, tax number or personal identification number (EMŠO), citizenship, and number, type and title of the issuer of the official identity document or company name, address, registered office and personal identification number of the person for whom there are grounds to suspect money laundering or terrorist financing; ☐
- ☐ Transaction, asset and property data for which there are grounds to suspect money laundering or terrorist financing (amount, currency, type of assets and property, value of assets and property, date or period of execution of transactions); ☐
- ☐ Grounds to suspect money laundering or terrorist financing; ☐
- ☐ For beneficial owners: a) personal name, address of permanent and temporary residences, date of birth, citizenship and share of ownership or other means of control; b) in the case referred to in point b) of paragraph one of Article 37 of this Act, information on the category of persons whose interest is the establishment and operation of a foreign trust, foreign institution or similar foreign law legal entity. ☐
- ☐ The name of the other civil law entity referred to in point 5 of Article 3 of the ZPPDFT-2 and personal name, address of permanent or temporary residences, date and place of birth and tax number or personal identification number (EMŠO) of the member. ☐

4.3.2 Simplified customer due diligence

If the customer, business relationship, transaction, product, service, distribution channel, country or geographical area pose a slight risk of money laundering or terrorist financing, you are required to carry out simplified customer due diligence.

In these cases, the ZPPDFT-2 allows for a reduction in the scope of the measures prescribed in the context of normal customer due diligence. The manner in which simplified customer due diligence is to be carried out is set out in Article 63 of the ZPPDFT-2. In carrying out simplified customer due diligence, it is necessary to also consider the results of the national risk assessment.

4.3.3 Enhanced customer due diligence

If a customer, business relationship, transaction, product, service, distribution channel, country or geographical area presents an increased risk, enhanced customer due diligence is required. In addition to the measures provided for as part of normal customer due diligence, additional measures are to be implemented.

The ZPPDFT-2 does not define the set of additional measures (see Article 64 et seq.); instead, the guidelines issued by supervisory authorities should be followed. In this context, the Bar Association of Slovenia recommends that lawyers and law firms, at their own discretion, request the submission of additional documents or define the implementation of additional measures to satisfactorily verify the data obtained on the customer and the intended nature of the business relationship.

In carrying out enhanced customer due diligence, it is necessary to also consider the results of the national risk assessment.

4.4 REPORTING DATA TO THE OFFICE (Article 75 of the ZPPDFT-2)

Lawyers and law firms must report to the Bar Association of Slovenia all cases in which a customer seeks advice for the purpose of money laundering or terrorist financing purposes immediately or no later than within three business days of the date the advice was sought (Article 90 of the ZPPDFT-2).

In all other cases, where lawyers and law firms carry out activities referred to in Article 90 of the ZPPDFT-2 (thereby becoming an obliged entity under the ZPPDFT-1), any cash transaction exceeding EUR 15,000 must be reported to the Office immediately upon execution, but no later than three working days after its completion (Article 75 of the ZPPDFT-2).

Suspicious transactions: Lawyers and law firms must report to the Office the data referred to in paragraph one of Article 150 of the ZPPDFT-2, along with the related documents, whenever there are grounds to suspect money laundering or terrorist financing in connection with a transaction, person, property or assets before the transaction is carried out, and specify in the report the time limit within which the transaction is intended to take place. Such a suspicious transaction report must be submitted to the Office via secure electronic means. Exceptionally it may be submitted by telephone; however, in such cases, it must also be submitted by secure electronic means no later than the next business day. The obligation to report suspicious transactions also applies to the intended transaction, whether or not it was subsequently executed (Article 76 of the ZPPDFT-2).

The aforementioned reporting obligation does not apply to lawyers and law firms with regard to data obtained from or concerning the customer while establishing the customer's legal position or when acting as the customer's representative in judicial proceedings, including providing advice concerning the institution or avoidance of such proceedings, irrespective of whether such data is obtained before, during or after such proceedings.

Under these conditions, lawyers and law firms are not obliged to send the data, information and documents to the Office; however, they are obliged immediately, and no later than within 15 days of receipt of the written request from the Office, to inform the Office in writing of the reasons for non-compliance with its request (Article 83 of the ZPPDFT-2).

The forms for reporting data to the Office are available [here](#). Please note that to submit reports using the new online forms, prior registration is required, which must be completed using a qualified digital certificate.

4.5 AML/CFT COMPLIANCE OFFICER, TRAINING AND INTERNAL CONTROL (Article 83 et seq. of the ZPPDFT-1)

4.5.1 AML/CFT COMPLIANCE OFFICER

Lawyers and law firms employing four or more persons must appoint an AML/CFT Compliance Officer and at least one deputy for the specific tasks of detecting and preventing money laundering and terrorist financing. The deputy acts on behalf of the AML/CFT Compliance Officer in their absence with regard to the full scope of tasks, and also performs other tasks under the ZPPDFT-2 if stipulated by the obliged entity's internal regulations.

Lawyers and law firms with fewer than four employees need not appoint an AML/CFT Compliance Officer.

If an obliged entity with fewer than four employees appoints an AML/CFT Compliance Officer and one or more deputies, these persons must meet the requirements referred to in Article 84 of this Act

and perform the tasks referred to in Article 85 of this Act. If an obliged entity with fewer than four employees still performs internal control, they must do so in accordance with Article 88 of this Act.

The obliged entities referred to in Article 4 of this Act who have branches and majority-owned subsidiaries established in third countries must appoint an AML/CFT Compliance Officer of the group and one or more deputies to carry out the tasks of detecting and preventing money laundering and terrorist financing provided by this Act and the ensuing regulations.

The AML/CFT Compliance Officer must meet the following requirements:

- ☐ They must be employed in a sufficiently high position to carry out duties quickly and efficiently (the placement of the AML/CFT Compliance Officer in the organisational structure is appropriate if they are guaranteed independence from other organisational parts, unrestricted access to data and information at the level of the entire office and the possibility of direct reporting to management – see Article 84 of the ZPPDFT-2);☐
- ☐ They must not have been convicted in a final judgment, nor be subject to criminal proceedings for a premeditated criminal offence or for specific criminal offences committed through negligence (negligent manslaughter, serious bodily harm, aggravated bodily harm, threatening work safety, concealment, disclosure and undue obtaining of professional secrets, money laundering, disclosure of classified data or causing general danger), and the sentence has not yet been expunged from the criminal record;☐
- ☐ They hold appropriate professional qualifications for the tasks required for preventing money laundering and terrorist financing;☐
- ☐ They have a thorough understanding of the nature of the obliged entity's operations in areas vulnerable to money laundering and terrorist financing risks.☐

The AML/CFT Compliance Officer's deputy is not required to meet the requirements for the AML/CFT Compliance Officer (employed in a sufficiently high position – Article 86 of the ZPPDFT-2).

Lawyers and law firms employing four persons or more must inform the Office of the personal name and job title of the AML/CFT Compliance Officer and their deputy and any changes thereof no later than in fifteen days following the appointment or the change of data.

The full and effective functioning of the anti-money laundering and terrorist financing system includes the following tasks of the AML/CFT Compliance Officer (Article 78 of the ZPPDFT-2):

- ☐ Ensuring the setting up, functioning and development of the obliged entity's system for detecting and preventing money laundering and terrorist financing;☐
- ☐ Ensuring the correct and timely reporting of data to the Office in accordance with the ZPPDFT-2 and regulations issued on its basis;☐
- ☐ Participation in the drawing up and modification of the operative procedures and in the preparation of internal regulations of the obliged entity concerning the prevention and detection of money laundering and terrorist financing;☐
- ☐ Participation in the development of guidelines for the conduct of control related to the of detection and prevention of money laundering and terrorist financing;☐
- ☐ Monitoring and coordinating the obliged entity's activities in the detection and prevention of money laundering and terrorist financing;☐

- Participation in the setting up and development of information technology support for activities related to the detection and prevention of money laundering and terrorist financing with the obliged entity; □
- Submitting initiatives and proposals to the management of the obliged entity to improve the system for detecting and preventing money laundering and terrorist financing; □
- Participating in the development of professional training and education programmes for the obliged entity's employees on money laundering and terrorist financing prevention and detection. □

The same system for preventing money laundering and terrorist financing must also be established in the branches of law firms as in the parent firm.

4.5.2 Professional training

Professional training is provided by lawyers and law firms to employees performing tasks related to the prevention of money laundering and terrorist financing, based on an annual professional training programme, which must be prepared by the end of March for the current year at the latest. The training includes education on relevant legislation and regulations adopted on its basis, professional literature, and lists of indicators for identifying customers and transactions where there are grounds to suspect money laundering or terrorist financing (Article 87 of the ZPPDFT-2).

Education must be continuous and include any changes to the law or other regulatory requirements, as well as changes to internal procedures and policies.

Education should be targeted, meaning that the content is tailored to the specific needs of employees in individual departments or areas. Information on possible money laundering and terrorist financing methods and techniques should also be targeted and aligned with the specific needs of employees.

Where possible, new employees should receive training in the prevention of money laundering and terrorist financing.

In the training of the AML/CFT Compliance Officer and their deputies, it is particularly important to cover any new forms, methods and trends in the prevention and detection of money laundering and terrorist financing, to monitor legal and regulatory developments, and to provide information on changes within the office that may affect the risk profile.

Lawyers and law firms should maintain records of the training provided (the date of the training, participants, the availability of training materials).

4.5.3 Internal control

Lawyers and law firms with fewer than four employees are not required to carry out internal control.

Lawyers and law firms must ensure regular internal control over the performance of their tasks of detecting and preventing money laundering and terrorist financing. A risk management culture must be established to ensure that employees are adequately committed to strictly following the procedures and policies defined by lawyers and law firms, in order to comply with legal requirements related to the prevention of money laundering and terrorist financing.

The complexity of the internal control system should align with the size of the law firm and the scope and nature of the business. Larger firms are expected to implement specific internal controls at the departmental level or within the specific areas they cover, in accordance with the scope and nature of

the business. These controls should address the specific risks present within each department or area of operation.

The internal control system must ensure the following:

- ☐ Compliance with the identified lawyer or law firm risk profile regarding the prevention of money laundering and terrorist financing; ☐
- ☐ An analysis of new and existing customers in relation to their exposure to the risk of money laundering or terrorist financing, as well as regular customer due diligence based on the assigned customer risk profile; ☐
- ☐ Consistency between the activities conducted and the specified customer risk profile; ☐
- ☐ Regular reporting to management on the status of the prevention of money laundering and terrorist financing compliance, including adherence to legal requirements, and timely reporting of any identified deficiencies, along with the measures taken to address them; ☐
- ☐ A clear definition of responsibilities within the prevention of money laundering and terrorist financing system; ☐
- ☐ Continuity in the implementation of the prevention of money laundering and terrorist financing system, regardless of potential organisational or personnel changes; ☐
- ☐ Consistency in complying with all regulatory requirements, with an appropriate response to potential legal changes. ☐

The law firm's management should formally approve the internal control in writing.

The Ministry of Finance will issue a set of rules with detailed provisions on the AML/CFT Compliance Officer, the manner in which internal control, data retention and data protection are carried out, as well as the keeping of records and the professional training of employees.

4.6 THE LIST OF INDICATORS TO IDENTIFY CUSTOMERS AND TRANSACTIONS FOR WHICH THERE ARE REASONABLE GROUNDS TO SUSPECT MONEY LAUNDERING OR TERRORIST FINANCING (Articles 92 and 93 of the ZPPDFT-2)

Lawyers and law firms must compile a list of indicators to identify customers and transactions for which there are grounds to suspect money laundering or terrorist financing. They are required to use this list when determining whether there are grounds to suspect money laundering, terrorist financing or other related circumstances.

In creating the list of indicators, lawyers and law firms must give special consideration to the complexity and scope of the transactions being carried out, any unusual patterns, amounts or links between transactions that have no apparent economic or lawful purpose and/or are inconsistent with or disproportionate to the usual or expected business activities of the customer, as well as other factors related to the customer's status and other characteristics. Based on these indicators, a suspicious transaction may be presumed to have occurred. The list of indicators serves as the primary guideline for employees in identifying suspicious circumstances concerning a particular customer, a transaction

executed by the customer or a business relationship being entered into. Therefore, everyone within the law firm must be familiar with these indicators and incorporate them into their work.

[A sample list of indicators](#)

4.7 DATA PROTECTION AND RETENTION AND RECORDS MANAGEMENT (Article 134 et seq. of the ZPPDFT-2)

4.7.1 Data protection

Data subject to prohibition on disclosure

Lawyers and law firms are prohibited from disclosing that the data, information or documents obtained will be communicated to the Office (point 1 of paragraph one of Article 134 of the ZPPDFT-1), that the Office requested the submission of data, that the Office halted the transaction or issued instructions to the lawyer or the law firm in this regard, that it requested ongoing monitoring of the customer's business, that it conducted an operational analysis of the customer or a third party, and that pre-trial or criminal proceedings have been or might be initiated against the customer or third party (paragraph one of Article 134 of the ZPPDFT-2).

When does the prohibition on data disclosure under the ZPPDFT-2 not apply?

The prohibition on disclosure does not apply in cases where lawyers and law firms attempt to dissuade a customer from engaging in unlawful activity, as such action is not considered disclosure within the meaning of the prohibition.

In addition, the prohibition does not apply to the disclosure of data (referred to in point 1 of paragraph one of Article 134 of the ZPPDFT-2) when such data are exchanged among lawyers and law firms operating within the same legal entity or network, provided they are established in Member States (i.e. disclosure of data within the network). In such cases, lawyers and law firms must maintain records of the disclosed data, which are not subject to the prohibition, and ensure that the data is processed in accordance with paragraph three of Article 134 of the ZPPDFT-2.

Furthermore, the prohibition on data disclosure does not apply to information that the data, information or documents obtained will be communicated to the Office, where such disclosure occurs between lawyers and law firms, provided that the following conditions are met:

1. The transaction relates to two or more of the persons concerned;
2. The transaction relates to the same customer;
3. The persons concerned are established in a Member State or in a third country that applies anti-money laundering and terrorist financing measures equivalent to those set out in this Act; 4. The persons concerned perform the same activity or belong to the same category of profession;
5. They are subject to obligations regarding the protection of professional and business secrecy and personal data (i.e. disclosure of data within the same categories). In such cases, lawyers and law firms must maintain a record of the data disclosed within the same categories, which is not subject to the prohibition on disclosure, and which pertains to the data referred to in paragraph two of Article 137 of the ZPPDFT-2.

Otherwise, lawyers and law firms must classify data subject to the prohibition on disclosure, as well as reports of suspicious transactions or information regarding other criminal offences (Articles 110 and 111 of the ZPPDFT-2), with the appropriate classification level in accordance with the Act governing classified data.

The obligation to protect classified data applies to all persons, including members of management bodies and others who may access such data by any means. Access to this data must otherwise be restricted.

When does the obligation to protect classified data under the ZPPDFT-2 not apply?

The obligation does not apply where such data, information or documents are required to establish facts in criminal proceedings, are requested in writing by a competent court, or are requested by the Bar Association of Slovenia for the purpose of supervising the implementation of the ZPPDFT-2.

The exemption from the obligation to protect classified data also applies when lawyers and law firms are required to submit such data to the Office in accordance with the ZPPDFT-2. In such cases, lawyers, law firms and their employees are not be held liable for any damage caused to the customer or a third party if the data were transmitted in compliance with the ZPPDFT-2 or upon request of the Office.

4.7.2 Data retention

Pursuant to the ZPPDFT-1, lawyers and law firms must ensure the proper retention of data. All data and related documents obtained pursuant to paragraph one of Article 142 must be kept for 10 years after the customer's identity has been established. Data and related documents concerning the professional training of employees must be retained for four years following the completion of the training.

4.7.3 Management of records

Pursuant to the ZPPDFT-2, lawyers and law firms must maintain at least the following records:

- ☐ Customer information; ☐
- ☐ Data on business relationships; ☐
- ☐ Data on transactions of EUR 15,000 or more; ☐
- ☐ On transactions reported to the Office (cash, suspicious); ☐
- ☐ On access to data subject to the prohibition on disclosure, by the supervisory body (the Bar Association of Slovenia). ☐

These records must contain all data required by law (content of records – Articles 150 and 151 of the ZPPDFT-2). Although the law does not prescribe a specific format (e.g. paper or electronic), it is recommended to maintain electronic records wherever possible, in order to enhance transparency and facilitate effective and consistent monitoring of business activities.

6. INSPECTION PERFORMED BY THE OFFICE – SPECIFICS REGARDING LAWYERS (Article 159 of the ZPPDFT-2)

Under the new arrangements, the Office also has the authority to carry out inspections. The ZPPDFT-2 contains specific provisions governing the supervision of lawyers and law firms by the Office.

The obliged entity must provide the inspector with access to the premises, books of account and other documents, and must not obstruct the inspection in any way, unless legal confidentiality is being exercised.

Inspectors responsible for the prevention of money laundering must notify the Bar Association of Slovenia in advance of the indicative time frame and the location of the intended inspection, in order to ensure the presence of its representative.

Lawyers and law firms subject to inspection have the right to request that the inspection be carried out in the presence of a representative of the Bar Association of Slovenia. Until their arrival, all inspection activities must be suspended, but for no longer than two hours from the moment the lawyer or law firm requests their presence. After this period, the inspection will proceed without the representative.

In the performance of their inspection duties involving a lawyer or a law firm, the anti-money laundering inspector is entitled to exercise all inspection powers under Article 159 of the ZPPDFT-2, unless the exercise of such powers would interfere with legal confidentiality.

A lawyer, law firm or the representative of the Bar Association of Slovenia, if present, has the right to object to the examination or seizure of data and documents in order to safeguard legal confidentiality. In the event of such an objection, the procedure will continue in accordance with the provisions of the Act governing criminal procedure, applied *mutatis mutandis*.

If the obliged entity refuses or obstructs the inspector's entry into the premises, denies access to books of account or other documents, or otherwise prevents or interferes with the conduct of the inspection, or where such interference may reasonably be expected, the inspector may enter the premises or access the books of account and documents against the will of the obliged entity with the assistance of the police, except where the obliged entity is a lawyer or a law firm. The costs of such entry or access, as well as any resulting damage, are borne by the obliged entity.

7. OFFENCE PROVISIONS RELATING TO LAWYERS AND LAW FIRMS

A law firm whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years may be fined between EUR 3,000 and EUR 60,000 for failing to notify the Bar Association of Slovenia within the prescribed time limit that it was approached by a customer seeking advice on money laundering or terrorist financing and for failing to decline to provide further advice to the customer (paragraph two of Article 90).

A law firm whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years may be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

A law firm whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years may be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph one of this Article.

Lawyers and notaries may be fined between EUR 2,000 and EUR 40,000 for failing to notify the Bar Association of Slovenia or the Chamber of Notaries of Slovenia, respectively, within the prescribed time limit that they were approached by a customer seeking advice on money laundering or terrorist financing and for failing to decline to provide further advice to the customer (paragraph two of Article 90).

A law firm whose accounts show revenue not exceeding EUR 700,000 on the balance sheet cut-off date for the last two consecutive financial years may be fined between EUR 3,000 and EUR 60,000 for the offence of failing to communicate to the Office within the prescribed time limit the required data, information and documents when there are reasons to suspect money laundering or terrorist financing in connection with a transaction, person, property or assets (paragraphs one, two and three of Article 100).

A law firm whose accounts show revenue exceeding EUR 700,000 and not exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years may be fined between EUR 6,000 and EUR 60,000 for committing the offence referred to in the preceding paragraph.

A law firm whose accounts show revenue exceeding EUR 8,000,000 on the balance sheet cut-off date for the last two consecutive financial years may be fined between EUR 12,000 and EUR 120,000 for committing the offence referred to in paragraph five of this Article.

Lawyers and notaries may be fined between EUR 2,000 and EUR 40,000 for the offence of failing to communicate to the Office within the prescribed time limit the required data, information and documents when there are reasons to suspect money laundering or terrorist financing in connection with a transaction, person, property or assets (paragraphs one, two and three of Article 100).

The responsible person of a law firm, lawyer or notary may be fined between EUR 800 and EUR 4,000 for the offence referred to in paragraphs one, four, five or eight of this Article.

8. WRITTEN DOCUMENTS UNDER THE ZPPDFT-2

In view of the above, a lawyer or a law firm must have at least the following written documents in accordance with the ZPPDFT-2:

- ☐ Customer risk assessment and customer risk assessment form;
- ☐ Internal rules on money laundering prevention, documents on the adoption of measures to mitigate and manage the risks of money laundering or terrorist financing in light of the risks identified in the risk assessment;
- ☐ A list of risk indicators;
- ☐ An internal control act (for firms with four or more employees);
- ☐ Customer knowledge form;
- ☐ Records under the ZPPDFT-2.