FMA

Finanzmarktaufsicht
Liechtenstein

FMA Instruction 2018/7 – General and sector-specific interpretation of due diligence law

Reference:	FMA I 2018/7
Addressees:	Persons subject to due diligence under Article 3(1) and (2) SPG
Publication:	Website
Enactment:	24 April 2018
Entry into force:	24 April 2018
Last amendment:	13 April 2022
Legal bases:	Article 1 SPG
	Article 2(1) SPG
	Article 3 SPG
	Articles 5 to 9 and 11(4) SPG
	Article 14 SPG in conjunction with Article 24 SPV
	Article 14(4) SPG in conjunction with Article 24a SPV
	Article 20 SPG in conjunction with Articles 27 to 29 SPV
	Article 21 SPG in conjunction with Articles 31 to 36 SPV
	Article 22(1) SPG
	Article 28(3) SPG
	Articles 6 to 11a, 18(2), 20, 22 SPV
	Article 14 SPV
	Article 21(2) SPV

Unofficial translation

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

FMA

Contents

FMA

I. General Part

1. General provisions

Based on Article 28(3) of the Law on Professional Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing of Terrorism (Due Diligence Act, SPG), the Financial Market Authority (FMA) may issue instructions interpreting the provisions of the SPG and the Ordinance on Professional Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing of Terrorism (Due Diligence Ordinance, SPV) as appropriate to each industry sector.

The content of this Instruction reflects the interpretation and practice of the FMA in connection with the exercise of due diligence and was prepared in cooperation with the industry associations.

The General Part contains provisions which in principle apply to all persons subject to due diligence. The Special Part sets out the sector-specific details. Both parts form an integrated document and must accordingly be read together.

2. Terminology

- **Identification** refers to the identification and verification of a person's identity by means of documents with probative value (Articles 6 et seq. SPG).
- A **professional basis** exists if, taking account of the overall view of criteria such as frequency, remuneration, amount of remuneration where applicable, amount of assets concerned, type of contract, contracting party, number of transactions, etc., it can no longer be assumed that the service is performed on a courtesy basis. For the qualification under due diligence law as a service performed on a professional basis, it is irrelevant whether the activity is carried out on a self-employed or non-self-employed basis.
- **Documents with probative value**
  - for natural persons (Article 7(1) SPV):

    Valid official identity document bearing a photography, specifically a travel document (passport, identity card) or driving license. A travel document is valid if it entitles the holder to enter the Principality of Liechtenstein at the time of identification and verification of identity.

    See the list of the Swiss State Secretariat for Migration:

    https://www.sem.admin.ch/sem/de/home/themen/einreise/faq.html#-620728190

    If the contracting party is unable to produce such a document from his or her home state, the contracting party must obtain a confirmation of identity from the competent authorities of the place of residence (Article 7(2) SPV).
  - for legal entities (Article 8 SPV):

    Documents with probative value include extracts from the Commercial Register, official certificates issued in Liechtenstein, etc., which are not more than twelve months old (Article 10(3) SPV).
- A **business relationship** is any business, professional or commercial relationship which is conducted in connection with the professional activities of the person subject to due diligence and which is expected, at the time when the contact is established, to exist for a certain duration in time (Article 2(1)(c) SPG).

  For example, the term "business relationship" is defined in FMA Communication 2017/3 on electronic reporting in accordance with due diligence law on the basis of:
  - the administered legal entity;
  - the insurance policy; or

- of the account master.

- **Occasional transactions** are operations and transactions, especially money exchange, cash subscription of medium-term notes and bonds, cash buying or selling of bearer securities and cashing of cheques, unless the operation or transaction is carried out via an existing account or custody account in the name of the customer (Article 2(1)(d) SPG).

  The term "account" is not limited to bank accounts.

  If these operations or transactions are effected within the framework of a business relationship as referred to in Article 2(1)(c) SPG, they are not considered occasional transactions. In this case, the provisions of due diligence law governing the (permanent) business relationship apply.

- A **third country** is a state that is not a member of the European Economic Area (EEA) (Article 2(1)(i) SPG), such as Switzerland.

- **Members of the executive body** are natural persons who are members of the management, the board of directors, the supervisory board, the managing board or persons in a comparable function (Article 2(1)(r) SPG). "Persons in a comparable function" means only those persons who have the same hierarchical status as the members of the management, the board of directors, etc. and have powers comparable to those of the members of the management, the board of directors, etc.

- The **responsible member of the executive body** for the purposes of Article 22(1) SPG is a member of the executive body as referred to in Article 2(1)(r) SPG who is responsible for compliance with the SPG and the SPV.

- The **contracting party** is in general the natural or legal person who places the order to establish the business relationship or to carry out the occasional transaction. For example, in the case of a (bank) account, this is the (legal) person in whose name the account is established; in the case of the formation of a foundation, this is the (legal) person who places the formation order. After the formation of a legal entity, the legal entity itself, represented by its bodies, is generally considered the contracting party.

3. Addressees (Article 3 SPG)

The SPG and the SPV apply to persons subject to due diligence. Article 3(1) to (2) SPG sets out who is covered by this term.

Some professions, such as professional trustees, real estate agents, persons trading in goods, and members of tax consultancy professions and external bookkeepers, are not in themselves to be considered to be subject to due diligence, but rather only when they carry out certain activities. More detailed provisions can be found in the Special Part applicable to the industry sector in question.

4. Territorial scope of application

The SPG and the SPV must always be applied if a person subject to due diligence as referred to in Article 3(1) or (2) SPG acts within the scope of Article 5(2) SPG or has a doubt or suspicion. The principle of territoriality applies as a general rule. Under that principle, Liechtenstein due diligence legislation is always applicable if activities within the meaning of Article 3(1) SPG are carried out in or from Liechtenstein.

5. Due diligence obligations

5.1 Scope and application of due diligence (Article 5(1) SPG)

The person subject to due diligence must in principle meet all due diligence obligations. According to Article 5(1) SPG, these are:

- identification and verification of the identity of the contracting party (Article 6 SPG);
- identification and verification of the identity of the beneficial owner (Article 7 SPG);
- identification and verification of the identity of the recipient of the distribution of legal entities established on a discretionary basis and the beneficiary of life insurance policies and other insurances with investment-related objectives (Articles 7a and 7b SPG);
- establishment of a business profile (Article 8 SPG); and
- supervision of the business relationship at a level that is commensurate with the risk (Article 9 SPG).

The extent to which due diligence obligations must be met depends on the risk inherent in the individual business relationship or occasional transaction. Under Article 10 SPG, simplified due diligence may be applied in cases of minor risk with reference to money laundering, organised crime and terrorist financing. In the event of increased or high risks within the meaning of Article 11 SPG, correspondingly enhanced due diligence must be applied. This is referred to as application of the risk-based approach, which is described in more detail in FMA Guideline 2013/1 on the risk-based approach under due diligence law.

The due diligence obligations referred to in Article 5 SPG represent only part of the obligations to be met under the SPG and the SPV. Other obligations in particular include those regarding the documentation of compliance with due diligence obligations, internal organisation, and the obligation to report to the Financial Intelligence Unit (FIU).

5.2 Identification and verification of the identity of the contracting party (Article 6 SPG; Articles 6 et seq. SPV)

The contracting party must be identified and verified both in a business relationship and in an occasional transaction. If, over the course of the business relationship, doubts arise concerning the identity of the contracting party, the persons subject to due diligence must repeat the identification and verification of the identity of the contracting party.

For natural persons, one-time identification is sufficient for all subsequent business relationships. The identification document, i.e. the document with probative value (confirmatory document), must continue to be valid within the meaning of Article 7 SPV for all business relationships subsequently entered into.

In all cases, the completeness of the due diligence files must be ensured so that, in particular, changes to the documentation can also be traced. It is permissible for documents relevant to several due diligence files, such as a copy of the original or of the certified copy of the confirmatory document, to be kept in a central location, provided that the central safekeeping is clearly evident from the due diligence file in question.

If the contracting party is a legal entity, the documents may not be more than twelve months old at the time of establishment of each new business relationship in order to ensure that they reflect the current circumstances (Article 10(3) SPV). However, here again it is sufficient to obtain the documentation only once for several business relationships, provided that the documents are not older than twelve months. The above provisions regarding the completeness of the documentation and central safekeeping apply here *mutatis mutandis*.

The information to be obtained and recorded under Article 6(1)(b) SPV includes the names of the bodies or trustees acting formally on behalf of the legal entity in the relationship with the person subject to due diligence. But only those persons need to be identified who specifically interact with the person subject to due diligence in the context of establishing the business relationship and represent the contracting party (e.g. those bodies which make the written declaration for the legal entity under Article 11 SPV) and not, for example, the entire management.

The persons subject to due diligence must ascertain that each person purporting to act on behalf of the contracting party is authorised to do so. This can be done, for example, by inspecting a power of attorney or an extract from the Commercial Register. The persons subject to due diligence must establish the identity of such persons by documentation of the information referred to in Article 6(1)(a) SPV and verify such particulars

by consulting a supporting document (original or certified copy). Documentation in the due diligence file must be ensured.

Copies of the original or of the authenticated copy of the supporting documents must be made, including a conformation under Article 10(2) SPV that the original or authenticated copy has been inspected. The copies must then be signed and dated and placed in the due diligence file (subject to central safekeeping).

The person subject to due diligence must sign and date the documentation used to identify and verify the identity of the contracting party. The use of an individualised stamp, including particulars such as the employee's abbreviation and initials, also counts as a signature.

The signature may also be executed by an employee of the person subject to due diligence, provided that such employee is authorised to do so in accordance with the internal organisation of the person subject to due diligence (e.g. by internal instructions). As a rule, the documentation should be signed by the employee who enters into the business relationship or is significantly involved in this process. If questions about the documentation arise during an inspection, the FMA may seek to establish contact with this employee. It must therefore be ensured that the signatory of the documentation is identifiable by an external third party (e.g. by stating the name in legible writing or typescript below the signature).

Another possibility is electronically "signed" documentation, in which case the authenticity of the "signature" must be guaranteed. This means that a signature cannot be executed by more than one person, but only by the signing employee or person subject to due diligence. Ways of circumventing this requirement must be excluded as far as possible. This also includes scenarios in which systemic precautions are used to automatically and immutably document by which employee a document was verified and when.

In all the above-mentioned cases, the signatory of the documentation must be identifiable by an external third party.

According to Article 9 SPV, confirmations of authenticity may be issued by a branch or group member company of the person subject to due diligence or by another person subject to due diligence referred to in Article 3(1)(a) to (i) SPG, a professional trustee, a lawyer, an auditor or an asset manager subject to the EU Anti-Money Laundering Directive or equivalent regulation and supervision (see Section IV Annex 1 of this Instruction). A confirmation of authenticity issued by a notary or other public body that customarily issues such confirmations of authenticity also meets the legal requirements.

The identification and verification of the identity of the contracting party may also be accomplished through the measures set out in the instruction on safeguards pursuant to Article 14 SPV.

5.3 Identification and verification of the identity of the beneficial owner, the recipients of a distribution and the beneficiary of life insurance (Articles 7 et seq. SPG; Articles 11 et seq. SPV)

The identification and verification of the identity of the beneficial owner is divided into two parts as follows:

- 1st step: Identification and verification of the identity of the beneficial owner
- 2nd step: Establishment and verification of beneficial ownership

The first step concerns establishment of the identity of the beneficial owner by the person subject to due diligence (Article 7(1) SPG). The beneficial owner must be identified and verified both in a business relationship and in an occasional transaction. For this purpose, the person subject to due diligence must obtain and record the information referred to in Article 6(1)(a) SPV and verify it through risk-based and adequate measures (e.g. by obtaining a copy of the passport). The documentation must be dated. Note that the beneficial owner must be a natural person, subject to a few exceptions set out in Article 3(1)(b)(2) and 3(1)(d) to (i) and Article 22b(3) SPV.

In principle, the beneficial owner is the natural person on whose initiative or in whose interest a transaction or activity is carried out or a business relationship is ultimately constituted. In the case of legal entities, this is also the natural person in whose ownership or under whose control the legal entity ultimately is situated (Article 2(1)(e) SPG). A more specific definition is provided in Article 3 SPV. For detailed questions regarding

the determination of the beneficial owner, FMA Communication 2015/7 on questions relating to the identification of the beneficial owner under the Due Diligence Act must be consulted.

In addition to identifying and verifying the identity of the beneficial owner, the persons subject to due diligence must take risk-based and adequate measures to satisfy themselves in a second step that this person is actually the beneficial owner. In this context, the focus is therefore not on identity as such, but on the verification of beneficial ownership. In the case of legal entities, this includes risk-based and proportionate measures to identify the ownership and control structure, which includes the requirement that the ownership and control structure must be understood by the person subject to due diligence.

The risk inherent in the business relationship or transaction determines the extent of the verification of beneficial ownership. In the case of business relationships and transactions with low risks, it is generally sufficient if the details of the beneficial owner are confirmed by signature in the form of a written declaration by the contracting party (Article 11(2) SPV). If normal, increased, or high risks are identified, in addition to the written confirmation referred to in Article 11 SPV, further measures are in any case required to verify beneficial ownership.

The person subject to due diligence must use the sources and documents to be consulted for clarification of the source of wealth and the source of funds (see Section 5.4.2) to check whether the information provided by the contracting party on beneficial ownership is plausible and conclusive. The totality of the ownership and control structure must be documented in the due diligence files and be comprehensible to third parties (e.g. in the form of an organisational chart or in another suitable manner).

It is crucial that the person subject to due diligence has no doubts as to the identity of the beneficial owners and their actual beneficial ownership and that the results of the own research are plausible. Any documents or research results that serve as plausibility checks must be included in the due diligence files. By way of exception, documents under company law may also be documented outside the due diligence files.

With regard to the identification and verification of the identity of distribution recipients, please refer to the guidance in the Special Part on service providers for legal entities under point 4.2, which apply exclusively to that professional category under the conditions set out in Article 7a(2) and (4) SPG.

With regard to the determination and verification of the identity of the beneficiary of life insurance policies, reference is made to the explanations in the Special Part for insurance companies, Section 2.3.

With regard to the completeness of the documentation in the due diligence files, the provisions on the identification and verification of the identity of the contracting party apply *mutatis mutandis*. Also in the case of the identification of the beneficial owner and distribution recipient, it must be possible for an external third party to identify which natural person has signed the documentation.

The identification and verification of the identity of the beneficial owner may also be accomplished through the measures set out in the instruction on safeguards pursuant to Article 14 SPV.

The forms in Annexes 1 and 2 of the SPV (Forms C, T, and D) shall be used to determine the beneficial owner and the recipient of a distribution. Please refer to FMA Communication 2015/7 with regard to the use of other forms (Forms V and Y).

5.4 Business profile (Article 8 SPG; Article 20 SPV)

5.4.1 General

The business profile is the basis for the ongoing monitoring of a business relationship and must therefore contain sufficient information to ensure adequate monitoring. The business profile must contain at least the information required under Article 20 SPV and must take into account the individual circumstances and risks of a business relationship.

The degree of detail depends on the individual risk classification of the business relationship. This means that the higher the risk of a business relationship, the more information must be available about the business relationship.

In any case – irrespective of the risk – the person subject to due diligence must, on the basis of the information provided, be able to identify any deviations or anomalies in relation to past experience with the customer and the customer's business relationship. In this context, the specific description of the economic background and the origin of the contributed assets plays a key role. If the contracting partner is a legal entity, the person subject to due diligence must understand the purpose as well as the business of such legal entity. Only a complete picture of the background of the business relationship enables the person subject to due diligence to identify connections with money laundering, predicate offences of money laundering, organised crime, or terrorist financing. In addition, the business profile must be sufficiently informative so that expert third parties – for example within the scope of a due diligence inspection – are also able to identify any anomalies in connection with executed transactions and so on after mere consultation of the business profile.

The business profile must enable the person subject to due diligence to identify deviations or anomalies in relation to past experience with the customer. For example, if it is possible to subsume every conceivable transaction under a business profile because the specifications in the profile are too generic, this is not sufficiently detailed (see FMA Complaints Commission resolution FMA-BK 2015/7, ON 16[1]). This is the case, for example, if an extremely indeterminate amount (e.g. CHF 50,000 to CHF 1 million) is stated with regard to the inflow/outflow of assets. As a general rule, it is certainly possible and useful to specify a certain bandwidth, provided that the profile is sufficiently informative in context. Accordingly, the bandwidth provided must also be sufficiently informative. In any case, it is crucial that the expected inflows and outflows are in line with the economic background of the contributor of the assets and with the information in the profile. Overly general information about the intended use without further specification (e.g. "expenses") is also considered too indeterminate.

Information about the origin of the assets that is not sufficiently informative is also considered to be inadequate. For example, it is not enough to simply state that the assets have been generated by "business activity" without providing further information on this activity. A mere statement that the customer is a "pensioner" without further information on the origin of the assets (e.g. due to long-standing business relationships established before retirement) is also considered to be insufficient. The scope of the available information is decisive in individual cases.

The profile must generally be more detailed with the increasing risk of the business relationship, and a plausibility check or verification of the information provided by the client must be performed in accordance with Section 5.4.2.

There are no specific formal requirements for the creation of the business profile. However, all relevant information must be collected and presented coherently in the due diligence documents. It is not enough if the relevant information can be found in various documents; instead, the business profile must be prepared in a way that is suitable for ongoing monitoring and comprehensible to third parties (see resolution FMA-BK 2014/2, ON 6). This principle also applies if the business profile is kept electronically. However, the necessary information may be compiled from other applications or databases in a central location. In addition, the business profile must be complete, dated, and signed, and the creator of the business profile must be identifiable to an external third party (see resolution FMA-BK 2015/7, ON 16). The provisions on signing the documentation when identifying the contracting party apply *mutatis mutandis*.

In the case of takeovers of mandates, but also mergers, acquisitions, or similar circumstances, in which business relationships are transferred to a new person subject to due diligence, it is permissible on an exceptional basis for the existing business profile to continue to be used if it complies with the provisions of due diligence law, is verified and (newly) dated and signed (see resolution FMA-BK 2015/1, ON 5).

[1] The cited decisions of the FMA Complaints Commission (FMA-BK) are in principle not published, but they may be requested from the FMA-BK in anonymised form.

5.4.2 Content of the business profile with respect to source of funds (SoF) and source of wealth (SoW)

5.4.2.1 Clarification of source of wealth (SoW) and source of funds (SoF)

Information on the source of funds (SoF) and the source of wealth of the effective contributor of the assets (source of wealth, SoW) form the basis for effective ML/TF monitoring. This information allows the person subject to due diligence to obtain an adequate picture of the client[2] and to verify whether the client's transactions and activities are consistent with what may be expected based on the resulting client profile. Discrepancies between the information provided by the client and information from other sources or discrepancies with the economic characteristics of persons with comparable backgrounds can be important indicators of suspicion of ML/TF and must never be disregarded, irrespective of the risk class of the business relationship.

5.4.2.2 Meaning of source of wealth (SoW)

Article 20(1) SPV sets out the information that must be included in the business profile of a business relationship. The documentation must include the financial background of the total assets, including occupation and business activity of the actual or effective contributor of the assets (Article 20(1)(d) SPG). This is referred to as source of wealth (SoW).

SoW refers in general to a description of the economic, business, and/or commercial activities that generated or significantly contributed to the client's total assets. It should be noted that the composition of wealth-generating activities may change over time. In some circumstances, the addition of new activities/facts contributes to the accumulation of additional wealth.

The purpose of collecting SoW information is not to determine the precise value of the client's total assets, but rather for the person subject to due diligence to record, understand, and roughly quantify (e.g. using meaningful asset ranges) the significant elements that contributed to the total assets or at least the majority of the assets. If the account holder is an asset management structure, this task refers to the effective contributor(s) of the assets.

In the FMA's view, the source of wealth can essentially be divided into two categories as a first step:

- Family/generational wealth

  This category includes all assets that were not generated by the client themself, but rather by (as a rule, related) third parties and were subsequently transferred to the client's assets. These are usually family assets that have been transferred to the client's assets through inheritance or gifts (from the family, including spouse/partner) or divorce agreements.

- Income, sales revenue, and business activity

  This category includes all assets generated by the client themself. This may include company property, business activity, employment, or the sale of products and other commercial assets.

  Examples of sources of wealth for natural persons are salaries, profit distributions, dividends, bonuses, commissions, and other compensation from employment or contractual work, as well as regular income from pension or retirement schemes.

  Examples of sources of wealth for operating companies are profits generated from their activities (e.g. sale of goods or services), receivables, contracts, available fixed assets, or financing.

Both (1) family/generational wealth and wealth from (2) income, sales revenue, and business activity can be used by the client to make further (3) investments.

[2] The term "client" includes the contracting party and the beneficial owner(s) or the effective contributor(s) (if not identical with the beneficial owner(s)) or the effective premium payer(s) (for insurance contracts).

The wealth may accordingly have been further increased by passive income resulting from the acquisition and sale of investments (e.g. real estate, securities, etc.). In the case of investment income, the source of the original investments must, from the FMA's perspective, always be comprehensible in the business profile.

The level of detail of the information on SoW must take into account the risk of the business relationship (see Article 20(2) SPV). The information may originate from the client and/or other sources, including any available public sources.

5.4.2.3 Meaning of source of funds (SoF)

In addition to the source of wealth, the origin of the deposited or contributed assets must be documented in the business profile (Article 20(1)(c) SPV). This information is referred to as source of funds (SoF).

SoF refers to the origin of the funds or assets contributed at the establishment and in the course of a business relationship. The assets contributed are a subset of the total assets. SoF generally represents one of several sources that make up the total assets (SoW). Consequently, the source of funds is usually easier to determine than the source of wealth.

However, the determination of SoF must not be limited to merely documenting from which bank or financial institution the funds originate or are transferred. Rather, the economic origin or creation of these specific assets must be explained. Furthermore, it must also be possible to trace the funds or assets in order to perform a plausibility check of the link between the economic background and the origin.

The mere fact that assets originate from a (different) bank account of the same client does not necessarily mean that their origin is legitimate, given that:

- the (other) bank may have filed a report of suspicion with the competent FIU with respect to such assets and received approval to transfer the assets while the FIU continues to analyse the report of suspicion, or
- the bank may not have carried out appropriate due diligence.

The level of detail of the information on SoF must take into account the risk of the business relationship (see Article 20(2) SPV). The information may originate from the client and/or other sources, including any available public sources.

5.4.2.4 Plausibility check of the information provided by the client on SoW and SoF

A plausibility check in this context means a rough check of the comprehensibility and coherence of the information received from the client, on the basis of publicly available information (internet research[3]) and/or on the basis of comparative experience and industry benchmarks. The client advisor's perceptions of SoW/SoF in the course of on-site client contacts can also serve to check plausibility (memorandum).

Examples of plausibility checks:

Example 1: The client is the owner and general manager of a mechanical engineering company located in Germany/Austria/Switzerland/Liechtenstein. The company is known beyond its region and has been operating for more than 30 years. The client would like to use private banking services for his private assets generated from the company profits. Media reports on the company and a professional website exist, which allow at least rough conclusions to be drawn about the size and turnover of the company. The person subject to due diligence also has corresponding experience in the industry and industry benchmarks at their disposal.

Example 2: The client is a foundation. The founder has been the chief physician for many years at a university hospital in Germany/Austria/Switzerland/Liechtenstein. The founder has transferred large parts of his private assets, generated from his professional activities, to a Liechtenstein family foundation. The beneficiaries are

[3] e.g. company website, other media reports (in contrast to the reports suitable for verification (point 5), these reports do not necessarily have to contain specific figures/quotas or data)

the client's descendants. Information is publicly available on average salaries at clinics in the client's country. This means that benchmarks are available to the person subject to due diligence. The activities of the client are documented on the website of the clinic.

5.4.2.5 Verification of the information provided by the client on SoF

"Verification" means evidence of a statement based on documents and third-party evidence from trusted sources (independent of the client).

In connection with verification of the source of funds, the following documents in particular may be of relevance by way of example:

- proof of income
- certificates of inheritance
- purchase contracts
- tax returns
- employment contracts
- extracts from the Land Register
- decisions on dividend distributions
- annual financial statements
- donation agreements
- loan agreements
- blockchain data in conjunction with further documents
- etc.

Provided that doing so provides meaningful information on the origin of the contributed assets, the verification of SoF can also be carried out using public sources (i.e. reputable internet sources and media reports such as Forbes lists, Bilanz ranking, Reuters).

Persons who hold important public offices in Liechtenstein, as well as the scope of regular income associated with such offices, are in many cases generally known in Liechtenstein (see, for example, the Salary Act and Ordinance, comparison of remuneration customary in the sector, etc.). In the case of domestic politically exposed persons, there is accordingly no need by default to verify client information on SoF, provided that there are no additional risk-increasing factors that would lead to an increased or high risk. If no such additional risk-increasing factors exist, a plausibility check as described above is sufficient.

This also applies to their immediate family members or persons known to be close associates of them (who are also considered domestic PEPs under Article 2(1)(h) SPG), unless they qualify as a business relationship with increased or high risks due to other factors. However, the need to obtain documents may arise in the course of ongoing monitoring for the purpose of clarifying facts and transactions that deviate from the business profile or that give rise to suspicions.

5.4.2.6 Checks relating to information provided by clients on SoW and SoF in the area of regular risks

In the area of regular risks, the FMA does not expect verification, but rather only a plausibility check of the information provided by the client on the source of funds (see Figure 1). No verification is expected for the information on source of wealth.

The precondition, however, is that the risk classification of the business relationship meets the legal requirements and that the information in the business profile is meaningful and comprehensible to a third party. The risk assessment must take into account the results of the National Risk Assessment and the risk factors set out in the annexes to the SPG and in Guideline 2013/1[4].

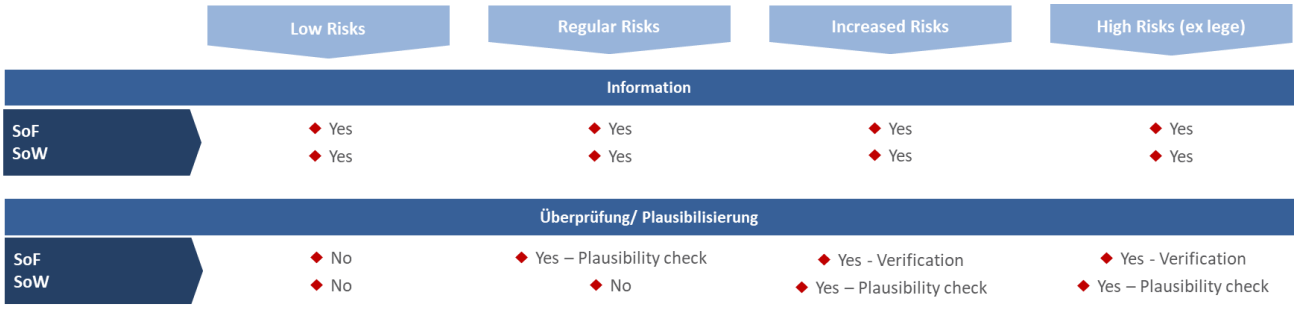
[4] In the case of risk assessment tools provided by the FMA, the risk assessment tool is decisive for the categorisation.

5.4.2.7 Checks relating to information provided by clients on SoW and SoF in the area of increased and high risks

In the area of increased and high risks, the FMA expects

- verification of the information provided by the client on source of funds, and
- a plausibility check of the information provided on the client's source of wealth.

Figure 1 – Overview of information and verification requirements



5.4.2.8 Dealing with business relationships where third-party evidence/sources are missing ("comply or explain" approach)

In principle, the standards outlined above also apply to existing clients. However, there may be cases where evidence or sources (no longer) exist for the SoF check. From the FMA's perspective, this may be the case in particular for long-standing business relationships (see Figure 2 for specific applicability over time).

On a case-by-case basis, the following questions must then be addressed and an assessment made as to whether and, if so, under which additional risk-mitigating measures the business relationship can be continued or entered into despite deviations from the applicable standards ("comply or explain" approach).

- For what reasons are no further documents or sources available and why can they no longer be obtained?
- What steps have been taken to obtain more information/documents?
- Is there nevertheless sufficient information to document SoF/SoW in a plausible and comprehensible way?
- What measures, if any, are being taken to mitigate the risk arising from the missing evidence/sources (e.g. intensified clarification of transactions)?
- What are the risk-increasing factors?
- Does negative information about the client exist (adverse media)?

The answers to these questions must be documented, and it must conclusively be determined whether, from the point of view of the person subject to due diligence, it is justifiable to maintain an account or business relationship or whether termination appears to be called for.

The following differentiation in terms of time must be observed for the treatment of existing clients and new clients.

New clients and existing business relationships from 1 January 2018

The importance of identifying and verifying SoF and SoW has always been emphasised in Liechtenstein due diligence law. With the implementation of the 4th Anti-Money Laundering Directive and the revision of the Due Diligence Act effective 1 September 2017, the associated strengthening of the risk-based approach, and further specification of the requirements in the FMA regulations, the importance of SoF and SoW measures has been given additional emphasis. In this context, there has in principle been no scope since 1 January 2018 for application of the "comply or explain" approach outlined above. Exceptions are permitted only in individual cases.

Exceptions are permitted only for business relationships

- that were already being serviced by another Liechtenstein person subject to due diligence before 2018,[5]
- for which sufficient information on SoF and SoW is available that has been subject to an adequate plausibility check, and
- for which the "comply or explain" approach was properly used in the context of this Instruction or which date from before 2001.

These conditions must be met cumulatively.

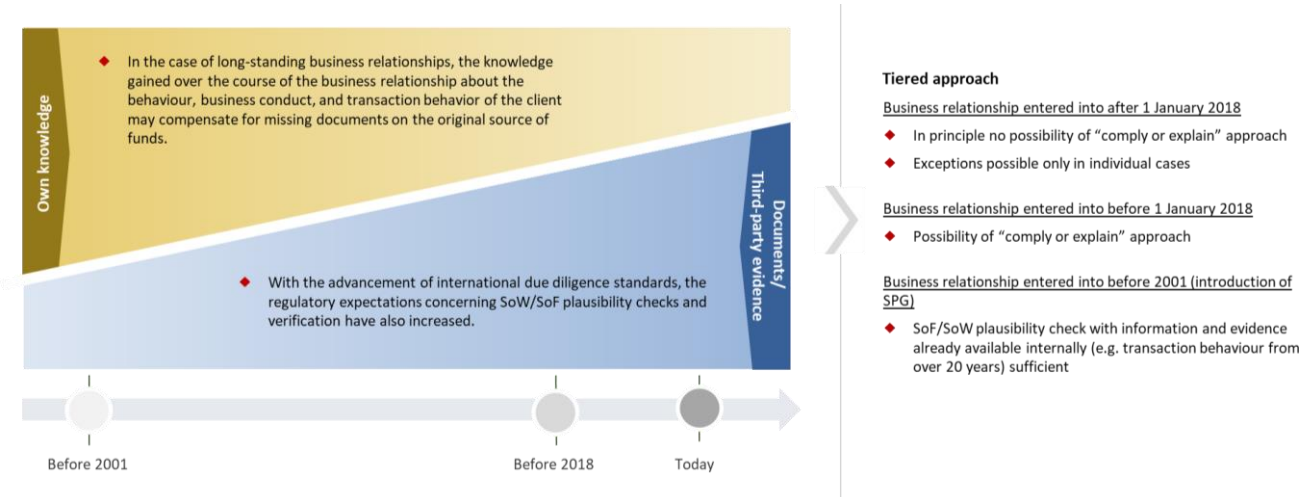
Existing business relationships before 1 January 2018

The FMA considers the application of the "comply or explain" approach outlined above to be permissible in connection with business relationships that were entered into before 1 January 2018. The plausibility check and verification requirements in relation to SoF/SoW were already explicitly in existence at that time, but they were not yet equally developed. Additionally, it can generally be assumed in such cases that the knowledge gained about the behaviour, business conduct, and transaction behaviour of the client in light of the long duration of the business relationship compensates for missing documents on the original source of funds.

Existing business relationships before 2001

In the case of business relationships entered into before the Due Diligence Act entered into force, the plausibility check of SoF/SoW using information and evidence already available internally (including transaction behaviour from over 20 years) may be sufficient.

Figure 2 – Requirements for existing clients and new clients



[5] This condition is also deemed to be met when entering into new business relationships with underlying companies of holding companies with which the person subject to due diligence already had a business relationship prior to 2018.

5.4.3 Updates of business profile

The business profile must always be kept current and must be actively updated at regular intervals by the person subject to due diligence (e.g. by contacting the contracting party, obtaining relevant documents, own research, inclusion of new facts).

The frequency of updates to the business profile depends on the risk. In any case, any changes relevant to the business profile or monitoring of the business relationship must be recorded.

In this context, there is an active obligation of the persons subject to due diligence to verify and update the entire portfolio of business relationships. The persons subject to due diligence must therefore regularly check whether all information and data to be collected within the scope of the business profile under Article 20 SPV still correspond to the actual circumstances.

For that reason, the business profile must be reviewed at individually defined, risk-appropriate intervals to ensure that it is up to date and adjusted if necessary. The frequency of the updates must be set out in the internal instructions or individual risk assessment (Article 31(2)(c^{bis}) SPV).

In cases of higher or high risks, the active review of the business profile must take place at least every one to two years, and in the case of normal risks at least every three to five years. In the case of low risks, the profile must be updated as warranted (e.g. when an "alert" is generated in the monitoring system). The specification of the update intervals is subject to known changes to the business profile. Known information that deviates from the existing business profile must therefore be taken into account immediately in the business profile.

When implemented in practice, the active obligation to review the business profile means that in the context of a client consultation, for example, questions must be asked specifically as to whether the information in the business profile (including beneficial ownership) still corresponds to the current circumstances. As a rule, the person subject to due diligence is already in a position to identify and document changes promptly on the basis of past knowledge of the client and generally close and regular client contact.

The update must be documented or recorded internally in accordance with Article 20(3) SPV. Provided that no changes are made when checking the need for an update, this result must be documented at least in the form of a short note or indication of the review. There is no explicit formal requirement in this respect. A short memorandum on the client consultation or a current dated printout of the profile are considered sufficient, as long as they contain the relevant information.

Any documents or research results which have served to check plausibility must be included in the due diligence file.

In the case of a plausibility check by means of supplementary deeds or comparable documents relating to beneficiary rules, mere inspection of such a document without making a copy is sufficient on an exceptional basis, in light of the sensitive nature of these documents. In such cases, the FMA expects the examination to be carried out in accordance with the principle of dual control and with appropriate documentation to be included in the due diligence file (date, persons inspecting the documents, contents of the documents inspected). For plausibility documents other than those mentioned above, mere inspection is not considered sufficient. Accordingly, the persons subject to due diligence involved in the business relationship must include them in the due diligence file.

5.5 Risk-appropriate monitoring (Article 9 SPG; Article 22 SPV)

Pursuant to Article 9(1) SPG, the persons subject to due diligence must carry out timely and risk-appropriate monitoring of their business relationships, including transactions executed in the course of the business relationship, in order to ensure that the course of the business relationship and the processing of transactions are consistent with the knowledge of the person subject to due diligence concerning the client and the client's business relationship and, consequently, correspond to the business profile (Article 8 SPG).

As is the case for other due diligence obligations, monitoring must be carried out in accordance with the risk categorisation. This means that in the case of a high or higher risk, continuous monitoring must be carried out more closely and in more detail than in the case of normal or even low risk. However, monitoring must always be carried out continuously and at regular intervals. The process for monitoring the business relationship must be regulated appropriately in the internal instructions or individual risk assessment under Article 9a SPG and brought to the attention of the employees who perform activities relevant to the due diligence obligations for daily use.

More detailed information on the specific requirements relating to risk-appropriate monitoring can be found in FMA Guideline 2013/1 on the risk-based approach under due diligence law.

5.5.1 Transaction monitoring

Under the legal requirements, transaction monitoring must be carried out in a timely manner, i.e. without delay after receipt of the transaction records or after knowledge of the transaction. After receipt of the transaction records (daily, monthly, or quarterly statements) or knowledge of the transaction, the transaction must be checked against the profile to determine conformity with the profile. In the case of business relations with increased or high risks, this check must be shown to take place within 14 days after receipt of the transaction records or after knowledge of the transaction [see Report and Motion (BuA) No. 159/2016, 67]. In other cases, i.e. for business relationships with a normal or minor risk, a period of 30 days for the check of a transaction against the profile is generally considered appropriate.

If the transaction does not correspond to the profile, a simple or, if necessary, a special investigation (Article 9 SPG; Article 22 SPV) must subsequently be commenced.

In addition, please note that cash transactions represent a higher risk from the point of view of combating money laundering than transactions by bank transfer. The risk of cash transactions must be taken into account by beginning the plausibility check at the time of their execution if they do not already correspond to the profile (e.g. payment of daily cash receipts from small and medium-sized enterprises). In general, downstream monitoring makes little sense and therefore does not meet the requirements of the SPG and the SPV in the case of cash transactions. This requirement is also justified by the fact that it is inherent to cash transactions that the customer is already present at the institution or service provider when such transactions are carried out.

The time intervals at which non-banks must obtain transaction records (daily, monthly or quarterly statements) and the threshold at which transaction monitoring is carried out must be specified by the person subject to due diligence in internal instructions or in the risk assessment for each risk category. The person subject to due diligence must be aware of the risks in connection with a business relationship and must set up monitoring accordingly. In any case, the timing of obtaining transaction records must be proportionate to the individual risk.

The process for monitoring the business relationship must be regulated appropriately in the internal instructions or individual risk assessment and brought to the attention of the employees concerned for daily use.

For a later review within the scope of transaction monitoring, for TT systems it is required to keep record of blockchain data, which allows the individual transactions and the transaction history to be traced using appropriate analysis tools.

5.5.2 Simple and special investigations (Article 9 SPG; Article 22 SPV)

As a consequence of risk-appropriate monitoring, the persons subject to due diligence are required under Article 9(3) SPG to carry out simple investigations with reasonable efforts when circumstances arise or transactions take place that deviate from the business profile. Pursuant to Article 22(1) SPV, the person subject to due diligence must obtain, evaluate and document the information that is appropriate to clarify and explain the background to such circumstances or transactions in this connection.

According to Article 9(4) SPG, special investigations must be carried out when circumstances arise or transactions take place giving rise to suspicion of money laundering, predicate offences of money laundering, organised crime, or terrorist financing. The indicators of money laundering, organised crime and financing of terrorism listed in Annex 3 of the SPV may also provide grounds for such investigations. The persons subject to due diligence may not discontinue the business relationship while these investigations are being carried out. In this context, the provisions of Article 18 SPG must be observed where applicable. According to Article 22(2) SPV, the person subject to due diligence must, in the context of special investigations, obtain, evaluate and document the information that is appropriate to eliminate or corroborate any factors giving rise to suspicions as referred to in Article 17(1) SPG.

In order to rule out deviations from the business profile or suspicious facts, the person subject to due diligence must obtain appropriate information within the meaning of Article 22 SPV so that the fact patterns or transactions in question can be checked for plausibility. As a result, the person subject to due diligence must be able to rely on the fact that no unclarified fact patterns or suspicions (any longer) exist. It is important to note that suspicions of money laundering or predicate offences of money laundering do not arise only once the person subject to due diligence has knowledge of a concrete predicate offence or the actual perpetrator of the predicate offence. See the case law of the Constitutional Court in this context,[6] according to which it is not necessary for the realisation of the elements of the crime of money laundering that the predicate offence from which the incriminated assets originate is proven with respect to place, time, perpetrator, modality, etc., let alone that it is or was established in a guilty verdict.[7] This must be done all the more at the level of special investigations, which are already triggered by mere suspicious facts. See also the case law on the suspicion threshold triggering the reporting obligation under Article 17(1) SPG and on the timeliness of notification to the FIU.[8]

Statements of the client in the context of clarification of a specific transaction clarification must be checked for plausibility. It is important to note that not every statement by the client can be accepted as is and without verification. Accordingly, depending on the case in question, (third-party) documents must be obtained to check the plausibility of the statement. In this context, please also note the provisions set out in Section 5.4.2 of this Instruction, which may be applied *mutatis mutandis*. The results of the investigations must be documented in the due diligence files in accordance with Article 9(5) SPG. The time period for the performance of a simple or special investigation is to be determined on the basis of the risk of the business relationship or the weight of the suspicion. A clear deadline can therefore not be specified, and a risk-based approach makes more sense. As a general rule, the more unusual and risky a transaction or fact pattern is considered to be, the more quickly the investigation should be carried out by the person subject to due diligence. According to case law,[9] special investigations under Article 9(4) SPG should not take months. If a constellation as described in the FIU guidance on the submission of reports of suspicion under Article 17 SPG (see more details under point 9 of this Instruction) arises, no further extensive investigations under Article 9(4) SPG are required, but rather a report of suspicion must be submitted under Article 17(1) SPG.

5.5.3 Media monitoring

Continuous monitoring at the risk-based level must also take into account media reports about clients that are relevant from the perspective of due diligence. Media reports are relevant in particular if the client is mentioned in connection with money laundering, predicate offences of money laundering, or organised crime. Insofar as such reports give rise to suspicion, these suspicions must be investigated in accordance with Article 9(4) SPG. If the suspicion cannot be dispelled, it must be examined whether there is an obligation to report in accordance with Article 17 SPG. The necessity and frequency of monitoring depends on the risk of the business relationship.

[6] See Constitutional Court judgment StGH 2014/152, § 8.4.
[7] See also Matthias Schmidle, Neues zur Geldwäscherei aus Wien und Strassburg, LJZ 2/2018, 78 et seq.
[8] See Court of Appeal judgment of 8. August 2018 in re 14 EU.2018.50, ON 35.
[9] See Court of Justice ruling of 3 December 2018 in re 13 EU.2018.142, ON 54.

For media monitoring (adverse media screening), either comparisons with databases of commercial providers or own searches in publicly available sources (e.g. Google) may be considered. In the case of databases of commercial providers, it is important to note that these databases often only provide for a comparison against PEP and sanctions lists. It must be ensured that the databases actually take media content into account to an appropriate extent (including media content from the relevant target markets). If the databases in use do not take current media content and open source content into account to an appropriate extent, this can be compensated for by internet research (e.g. World-Check basic version in combination with manual Internet research).

The performance of the inspections, the results and any clarifications made must be documented. If there are no relevant reports on a business relationship, a relevant note must be recorded and/or the printout of the first search results page must be kept on file with regard to the possibility of exculpation. The absence of relevant media reports does not have to be documented separately when using IT-based systems. Documentation via the log file is sufficient in this case.

Adverse media screening must be carried out at least in the following cases:

- During onboarding processes
- Risk-based, in the frequencies provided for updating the business profiles (see 5.4.2)
- Event-based, in case of changes in risk-relevant indications (e.g. change of BO, etc.)

For retail clients, no adverse media screening is expected (standardised private client business in the banking or insurance sector).

Especially in the case of persons subject to due diligence with a high number of business relationships, automated IT support should be sought in media monitoring.

6. Check with regard to politically exposed persons (PEPs) (Article 11(4) SPG)

According to Article 2(1)(h) SPG, PEPs are individuals who hold important public office or have held such office up to one year ago and also include their immediate family members and persons known to be close to them (known close associates). Only persons who perform functions at the level of the state are considered PEPs. Members of regional or cantonal parliaments, mayors, honorary consuls, etc., are therefore not considered PEPs. Whether, in addition to actual PEPs within the meaning of Article 2 SPV, other persons in public offices or serving the public interest should be treated analogously (in particular former PEPs at the end of one year after they are no longer in office) and thus classified as business relationships with increased or high risk is left to the individual risk management of the person subject to due diligence under Article 11(1) SPG.

Known close associates are persons who:

- are known to be joint beneficial owners of a legal entity with a PEP or have other close business relationships with a PEP (Article 2(3)(a) SPV);
- are the sole beneficial owner of a legal entity that is known to have been established for the benefit of a PEP (Article 2(3)(b) SPV); and
- are closely connected socially or politically with a politically exposed person (Article 2(3)(c) SPV; e.g. persons with whom a relationship is maintained (friend; life partner); prominent members (who are publicly perceived as spokespersons or who contribute to the shaping of opinion within the party in a way that can be perceived externally) of the same political party or business partners.

When determining the known close associate, the type, quality and timeliness of the connection with the politically exposed person must be taken into account. The number of close associates is fluid and may change over time. Thus, it may become apparent from the specific circumstances that persons who are identified as known close associates are not, or are no longer, in such a close relationship with a PEP. Such circumstances may arise in particular as a result of separation, estrangement or the termination of a business

relationship between the close associate and the PEP (paragraphs 46 et seq. FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)).

If a person subject to due diligence determines that he or she is providing financial services to a person closely associated socially or politically with a PEP, the person must be classified as a PEP and the required (enhanced) due diligence measures must be applied.

Persons subject to due diligence who use recognised commercial databases (which also contain media content from the respective target markets) for the PEP check and media monitoring can generally be confident of finding known close associates as defined above in such databases during the screening process. When establishing a business relationship or carrying out an occasional transaction, the person subject to due diligence must verify whether the contracting party or the beneficial owner is a PEP or not (PEP check). The person subject to due diligence must meet this obligation without delay, namely immediately upon establishing the business relationship or carrying out the occasional transaction (see resolution FMA-BK 2015/1, ON 5). Only in this way can the obligations under Article 11 SPG be met if it is determined whether a business relationship or an occasional transaction with a PEP exists in the first place. In addition, the person subject to due diligence must ensure a regular PEP check of the entire client base in order to ensure the identification of PEPs within the framework of existing business relationships. This regular PEP check must be carried out at least once a year.

The PEP check also applies to recipients of a distribution as referred to in Article 2(1)(p) SPG. In principle, the PEP check must take place at the time of payout of the distribution. However, persons subject to due diligence who are informed about the identity of the recipient of the distribution by other persons subject to due diligence pursuant to Article 7a(3) SPG do not have to carry out a PEP check until they have been informed.

Both the PEP check (including negative results, subject to the exception in the next paragraph) and the consent of at least one member of the executive body to the establishment or continuation of business relations with PEPs must be documented in the due diligence file (see resolution FMA-BK 2015/1, ON 5).

In the case of persons subject to due diligence who use an automated, computerised system for identifying business relationships and transactions with PEPs (Article 21(1) SPV), the documentation of negative results of the PEP check may on an exceptional basis take place at a central location (physically or electronically). In such a case, the person subject to due diligence must ensure that the PEP check is assigned to the proper due diligence file. On request, proof that a PEP check has been carried out for certain persons must be provided without unnecessary delay, so that the negative result can be presented directly. Positive results must accordingly be documented in the due diligence file.

Effective 1 June 2018, persons subject to due diligence must use an automated, computerised system (e.g. World-Check, Factiva, Pythagoras) to identify business relationships and transactions with PEPs if they have in excess of 100 business relationships under their management (Article 21(1) SPV).

More detailed information on politically exposed persons can be found in FMA Guideline 2013/1 on the risk-based approach under due diligence law.

7. Timing of due diligence obligations

Due diligence obligations must be performed in the cases referred to in Article 5(2) SPG, including when establishing a business relationship. A business relationship is deemed to have been established if activities relevant to due diligence law are carried out, e.g. by establishing/forming a legal entity, signing a declaration of acceptance, constituting a body, opening a (bank) account, obtaining signatory powers on the (bank) account, but not merely by conducting preliminary talks or issuing a formation order prior to acceptance by the person subject to due diligence.

If the due diligence obligations cannot be met, the person subject to due diligence may not establish the business relationship or carry out the desired transaction and must verify whether a report under Article 17 SPG is necessary. Likewise, an existing business relationship must be discontinued if the due diligence

obligations cannot be performed. In such cases, the discontinuation must be accompanied by sufficient documentation of the outflow of assets. This does not affect any reporting obligations under Articles 17 to 19 SPG.

The discontinuation of an existing business relationship takes precedence over other statutory or contractual provisions (Article 5(3)(b) SPG).

If the person subject to due diligence has doubts concerning the identity of the contracting party or the beneficial owner, the person subject to due diligence must repeat the identification. If doubts persist, but no suspicion arises within the meaning of Article 17 SPG (otherwise see procedure set out in Article 15(2) SPV), and the person subject to due diligence therefore terminates the business relationship, outward movements of assets shall be permitted only if proper records are kept. This allows the competent authorities to trace the assets further if necessary. In such a case, the person subject to due diligence may not disburse money in cash or physically surrender securities and precious metals, unless the contracting party has fully met the obligations and the documentation is complete.

Article 18(2) SPV sets out that in cases where this is necessary to maintain the normal conduct of business and there is a low risk of money laundering and terrorist financing as referred to in Article 10 SPG, the person subject to due diligence shall carry out the verification of the identity of the contracting party or beneficial owner as soon as possible after the first contact and ensure that no outward movement of assets takes place in the meantime.

Each case must be assessed individually. In no case may an outward movement of assets occur without the necessary documentation.

What should be considered "normal conduct of business" as referred to in Article 18(2) SPV depends on the individual case. Cases are conceivable, for instance, in which the travel document has already expired when the business relationship is established and no longer entitles the holder to enter the Principality of Liechtenstein. "Normal conduct of business" does not exist, for example, if there are doubts about the contracting party's information concerning the beneficial owner or the business profile.

8. Delegation and outsourcing of due diligence obligations

8.1 Delegation (Article 14 SPG, Article 24 SPV)

In principle, a person subject to due diligence may delegate due diligence obligations referred to in Article 5(1)(a) to (c) SPG to:

- another (domestic) person subject to due diligence; or
- a natural or legal person domiciled in another EEA Member State or third country:
    - whose due diligence and recordkeeping requirements meet the requirements set out in the EU Anti-Money Laundering Directive;
    - whose compliance with these requirements is supervised in a way that is consistent with Chapter VI Section 2 of the EU Anti-Money Laundering Directive; and
    - who is not domiciled in a state with strategic deficiencies as referred to in Article 2(1)(u) SPG.

The "other person subject to due diligence" is a (domestic) person subject to due diligence in accordance with Article 3(1) and (2) SPG. If due diligence obligations are to be delegated to an "other person subject to due diligence", the person subject to due diligence must check, for the purpose of the duty of due diligence of the (intended) delegate, whether the category of institution or profession of the latter is mentioned in the catalogue set out in Article 3(1) and (2) and whether any required licence is available (e.g. by inspecting the FMA register of licence holders). If the performance of certain activities is a prerequisite for due diligence (e.g. in the case of professional trustees, members of tax consultancy professions, and external bookkeepers and other persons subject to due diligence referred to in Article 3(3) SPG), a confirmation from the FMA on the duty of due diligence of the (intended) delegate must be obtained.

The EEA Member States are *de jure* obliged to implement the due diligence and recordkeeping requirements laid down in the EU Anti-Money Laundering Directive and the supervisory requirements laid down in Chapter VI Section 2 of the EU Anti-Money Laundering Directive. It can therefore be assumed that the systems for combating money laundering and terrorist financing in the EEA Member States meet the requirements of Article 14(1)(b)(1) and (2) SPG (equivalence of due diligence and recordkeeping requirements and supervision). To that extent, it is not necessary to verify the equivalence of the due diligence, recordkeeping, and supervision obligations applicable in another EEA Member State. When assessing equivalence, the current version of the list of countries in Section IV Annex 1 of this Instruction applies.

In all cases, however, the persons subject to due diligence must check themselves whether the (intended) delegate domiciled in an EEA Member State or a third country is actually subject to the due diligence and recordkeeping obligations and supervision of the competent authority of the country in question (e.g. by obtaining confirmation from the local supervisory authority or by inspecting public registers, where they exist). In the case of auditors, external bookkeepers, tax consultants, real estate agents, notaries, and other self-employed members of the legal consultancy professions, supervision by a self-regulatory body is also sufficient (see Article 48(9) of the EU Anti-Money Laundering Directive).

It must also be borne in mind that the delegate may not be domiciled in a state with strategic deficiencies as defined in Article 2(1)(u) SPG, even where that state meets the requirements under Article 14(1)(b)(1) and (2) SPG. In this context, please refer to the states with strategic deficiencies enumerated in Annex 4 SPV.

Persons subject to due diligence who avail themselves of third parties in this sense must ensure, in accordance with Article 24(1) SPV, that the data and documents collected by the third party under the SPG and SPV are transmitted to them immediately, and that the delegate confirms by signature that the copies produced conform to the originals or authenticated copies.

Even in the case of delegation, the responsibility for proper compliance with due diligence obligations always remains with the person subject to due diligence. There is no possibility of reducing the culpability of the person subject to due diligence.

The delegation is characterised by the fact that the due diligence obligations under Article 5(1)(a) to (c) SPG are exercised by a third party (see Articles 25 et seq. of the EU Anti-Money Laundering Directive). It should be noted in this regard that the third party may not act as a contracting party in the business relationship, otherwise inadmissible self-identification would occur.

The delegation must be documented, for example by a written delegation agreement. Further delegation (sub-delegation) by the delegate is not permitted.

In this context, it should be recalled that the provisions concerning delegation do not apply where persons subject to due diligence themselves obtain all documents and information required under the SPG and SPV (with or without personal contact).

Risk-appropriate monitoring of the business relationship as referred to in Article 5(1)(d) SPG is excluded from delegation.

8.2 Outsourcing (Article 14(4) SPG, Article 24a SPV)

Under certain conditions, both risk-appropriate monitoring as well as the identification and verification of the identity of the contracting party and the beneficial owner and the drawing up of the business profile may be contractually transferred to an outsourcing service provider. Article 24a SPV sets out the minimum requirements for effective outsourcing.

In this context, outsourcing of risk-appropriate monitoring analogous to delegation may be considered only if the outsourcing service provider is another person subject to due diligence under the SPG or a natural or legal person domiciled in another EEA Member State or third country under Article 14(1)(b) SPG. When verifying these conditions, the guidance under point 8.1 on delegation applies *mutatis mutandis*.

Outsourcing may occur under certain circumstances within a corporate group, but the arrangements in the individual case are always decisive.

The basis for outsourcing is a contractual agreement according to which the outsourcing service provider is to be regarded as part of the person subject to due diligence.

Finally, a clear distinction must be made between an outsourcing relationship and a delegation relationship.

9. Obligation to report to the FIU

Where suspicion of money laundering, a predicate offence to money laundering, organised crime, or terrorist financing exists, the persons subject to due diligence must immediately report to the Financial Intelligence Unit (FIU) in writing in accordance with Article 17(1) SPG.

In this connection, responsibility for submitting reports lies with the (responsible) member of the executive body appointed to ensure compliance with the SPG.

In this regard, see also the provisions set out in the guidance on the submission of suspicious activity reports to the FIU pursuant to Article 17 SPG: https://www.llv.li/files/sfiu/20170925-fiu-wegleitung-konsolidiert.pdf.

10. Reporting of unlawful acts

Under Article 28a(3) SPG, persons subject to due diligence having 100 employees or more who are involved with business relationships must create an internal whistleblower system through which employees can report violations of due diligence law via a special, independent, and anonymous channel.

Persons subject to due diligence which already have such an internal reporting system under the provisions of special legislation may use it for the purposes of the SPG.

In addition, the FMA has established a central reporting system under Article 28a(1) SPG by means of which potential or actual violations of due diligence law can be reported. Further information can be found on the FMA's website: https://www.fma-li.li/en/client-protection/whistleblowing.html

11. Documentation and internal organisation

11.1 Documentation (Article 20 SPG; Articles 27 to 29 SPV)

Under Article 20(1) SPG, the persons subject to due diligence must keep a record of compliance with the due diligence obligations set out in Articles 5 to 16 SPG and the reporting obligation set out in Article 17 SPG as provided in the SPG. They shall establish and maintain due diligence files for this purpose.

Under Article 27(1) SPV, the due diligence files must contain, in particular, the records and vouchers issued and consulted in order to comply with the provisions of the SPG and the SPV. In addition to the documents and records that have been used to identify and verify the identity of the contracting party and the beneficial owner, the business profile, and the transaction records, the due diligence files must also contain documentation concerning any investigations conducted in accordance with Article 9 SPG and all documents, records and vouchers consulted in this connection. The reasons for any application of simplified or enhanced due diligence pursuant to Articles 10 and 11 SPG must also be documented in the due diligence files. As an alternative, these reasons may also be documented in other suitable internal documents, such as the list of mandates or a risk matrix.

According to Article 28(1) SPV, the due diligence files must be kept in such a way that they enable third parties with specialist qualifications to make a reliable judgement concerning compliance with the provisions of the SPG and SPV. Under paragraph 2 of the same article, they may under certain conditions be stored in writing, electronically or in another similar format.

With reference to the requirements for electronic storage set out in Article 28(2) SPV, it is possible for due diligence files to be kept entirely in electronic form without the originals of certain documents such as, for example, identification documents having to be physically stored at the same time. These documents can be destroyed once they have been digitised. On a supplementary basis, see also Article 28(3) SPV, according

to which the integrity and legibility of the image and data storage media must be subject to regular checks. Ideally, a backup copy of the electronic data storage media is made in order to ensure access at all times. Furthermore, in the case of electronic storage, the examination of the records may not be more onerous or take up more time than the examination of the underlying documents.

The relevant information must be collected, prepared, and documented in the due diligence files. If a third party with specialist qualifications has to piece the information together first, this does not permit a reliable judgement to be made concerning compliance with the provisions of the SPG and the SPV (see resolution FMA-BK 2014/2, ON 6).

In summary, the due diligence files must be kept in such a way that a third party who is familiar with the provisions of the SPG and the SPV can without difficulties obtain an overview of the business relationship and its risks. In particular, this means that information with which the employees of the person subject to due diligence are familiar due to their personal background must both be included in the due diligence file and prepared in such a way that it is legible and comprehensible for an external third party. This also means in particular that the due diligence files must in principle be kept in German. Basic documents (e.g. application to open an account, forms for identifying the contracting party and beneficial owner) may be included in foreign languages. However, the relevant passages of documents which serve to check the plausibility of information and transactions and which were submitted by the customer in a foreign language other than English must be translated into German or English so that the statements made therein can be checked by a third party. As needed, the FMA may also order the translation of English documents into German.

The due diligence files must be held at a storage site in Liechtenstein that is accessible at all times (Article 28(5) SPV). The reason for this is that the competent domestic supervisory authorities must be guaranteed access at all times. In the case of electronic storage of due diligence files, it is permissible for the storage system ("server") to be located abroad, but it must be ensured that the data of the due diligence files are always available in up-to-date form in Liechtenstein. This can be done, for example, through regular synchronisation and storage of the data in Liechtenstein.

11.2 Internal organisation (Article 21 SPG; Articles 31 et seq. SPV)

The persons subject to due diligence shall take the necessary organisational measures and provide appropriate internal instruments of control and monitoring. They shall in particular issue internal instructions, arrange secure storage of the due diligence files, and arrange for training and development of their staff.

As appropriate to the circumstances and the individual risks, the internal organisation shall be structured according to the type and size of the enterprise as well as according to the number, type, and complexity of the business relationships. The effective fulfilment of the internal functions and due diligence requirements must be guaranteed at all times.

An appropriate internal organisation is characterised by a suitable organisational and operational structure. The organisational and operational structure must be designed in a risk-based manner. The larger, more complex and riskier the person subject to due diligence, the more stringent the requirements. The organisational and operational structure contains clear structures and reporting lines according to the “tone at the top” principle[10] (organisational chart), relevant competence regulations as well as appropriate control and monitoring structures. The relevant units (first, second and third lines of defence[11]) must be equipped with sufficient human and technical resources and powers to enable them to perform their tasks in the context of combating money laundering and preventing terrorist financing. Furthermore, it must be ensured in terms of organisation that the second line of defence is involved in all relevant processes (e.g. product development, contracting, etc.). An appropriate organisational and operational structure forms the basis for the effective fulfilment of due diligence obligations.

Furthermore, the inspection and monitoring measures are also part of the procedures and strategies (internal directives). These must specify how the investigating officer is to carry out the inspections and monitoring

[10] The “tone at the top” principle describes a corporate culture in which, in the present context, compliance is practised by the management level.
[11] For the definitions, see the explanations under Section 11.2.3.

measures. Depending on the size and complexity, a risk-based approach may be chosen, according to which not all areas of the company that are related to due diligence are subject to an annual audit obligation. This is also coupled with the implementation of an internal control system (ICS), which is characterised by the implementation of a random dual control for manual processes on the one hand and relevant risk-based monitoring of technical processes to determine whether the technical processes are still appropriate (that is, they comply with current technical standards) and effective (that is, a circumvention of the technical process is effectively prevented) on the other. The ICS and the second line of defence are always part of the annual audit cycle of the third line of defence in order to be able to make a fundamental statement about the effectiveness of the defence system.

11.2.1 Internal instructions (Article 21(1) SPG; Article 31 SPV)

The persons subject to due diligence shall draw up internal directives. In the internal directives to be issued by them, the persons subject to due diligence shall, in particular, specify appropriate strategies, procedures and controls and explain how the obligations under the due diligence legislation are specifically fulfilled and complied with. In their design, they must take into account the nature and complexity of the business activity of the person subject to due diligence. The internal directives must contain at least the information according to Article 31 SPV; in addition, they must also specify how the inspection and monitoring measures, in particular those of the investigating officer (Article 35 SPV), are carried out. The internal directives must be brought to the attention of the employees and issued by the management level.

The directives must be designed in such a way that they can serve as a guideline for the employees who perform activities relevant to the due diligence obligations. As a rule, it is therefore not sufficient for the instructions to merely reflect the text of the SPG or SPV. Rather, the persons subject to due diligence must formulate the internal instructions specifically for their business activities.

11.2.2 Training and development (Article 21(1) SPG; Article 32 SPV)

The persons subject to due diligence shall ensure that their employees who carry out activities relevant to due diligence receive up-to-date and comprehensive training and development. Relevant are, in particular, employees who are directly involved in business relations or who support such employees in their activities, employees who carry out advisory, inspection and monitoring measures, employees who have contact with clients, employees who have contact with client assets and persons performing management functions. This includes, in particular, the first, second and third lines of defence. The limit of the obligation to provide training and development must be drawn in relation to employees who do not perform activities relevant to due diligence (e.g. cleaning staff). This shall include instruction on the regulations for the prevention and combating of money laundering, predicate offences to money laundering, organised crime and the financing of terrorism as well as data protection law. At least the following topics must be covered:

- the obligations arising from the SPG and the SPV;
- the relevant provisions of the Criminal Code;
- the internal instructions;
- the conveyance of knowledge that will enable the employees to recognise transactions that are possibly connected with money laundering, organised crime or terrorist financing and to act correctly in such cases;
- the relevant provisions of data protection legislation.

Ideally, persons subject to due diligence and their employees attend external training and development events. It is of course permissible for the contents of external events to be passed on subsequently as part of internal training.

11.2.3 Internal functions (Article 22 SPG; Articles 33 et seq. SPV)

The persons subject to due diligence shall appoint a contact person for the competent supervisory authority as well as persons or specialist units for the internal functions of compliance officers and investigating officers.

In addition, a member of the executive body must be appointed who is responsible for ensuring compliance with due diligence law. The objective of this rule is to generate the strongest possible commitment to combating money laundering in the highest bodies of a legal entity. Accordingly, the FMA understands the term "persons in a comparable function" as referred to in Article 2(1)(r) SPG to mean only those persons who have the same hierarchical status as the members of the management, the board of directors, etc., and have powers comparable to those of the members of the management, the board of directors, etc. For example, a head of compliance who heads the compliance department and has the necessary and sufficient powers, but is not also a member of the general management, does not meet the qualification of the responsible member of the executive body. If no general management exists, at least the same hierarchical status as the board of directors or other equivalent body is required.

The responsible member of the executive body must have an in-depth knowledge in matters of the prevention and combating of money laundering, predicate offences of money laundering, organised crime and terrorist financing as well as data protection law, and be familiar with the current developments in those fields. Furthermore, the responsible member of the management level shall also be familiar with the company-wide organisational and operational structure in order to enable appropriate oversight of the performance of tasks by the second and third lines of defence. In this context, the monitoring of the second line of defence goes beyond reporting obligations. This person must also be provided with sufficient powers to ensure compliance with due diligence law by the person subject to due diligence (Article 36(1) and (2) SPV). If the person subject to due diligence can be accused of a monitoring failure or deficient organisation, the competent member of the executive body can be held criminally responsible (Article 33(1) SPG). In particular, it must be ensured that this person has free access to all information, data, records and systems which the person needs to perform his or her duties. The person must be able to stop transactions, block accounts, and order other such measures. The person must also have the right to veto the establishment of a business relationship or be able to enforce the discontinuation of such a relationship. This person is furthermore responsible for submitting suspicious activity reports to the FIU within the meaning of Article 17(1) SPG.

The compliance officer and the investigating officer must also be given access to the due diligence files at any time to enable them to perform their duties. In addition, these function holders must have an in-depth knowledge in matters of the prevention and combating of money laundering, predicate offences of money laundering, organised crime and terrorist financing as well as data protection law, and be familiar with the current developments in those fields. If a specialist unit is appointed for the functions of the compliance officer or investigating officer, the persons carrying out the work must likewise fulfil the described qualifications under due diligence law. In addition, a third party with specialist qualifications within the meaning of Article 28(1)(b) SPV must at all times be able to identify the persons by whom the tasks have been performed, for example by means of recognisable signature of the underlying documentation.

One person or a specialist unit, if applicable, may perform several functions, provided that implementation of the SPG is ensured. The functions of the compliance officer and the investigating officer should in principle be assigned to different persons in order to ensure a separation of duties. One of these two functions can also be performed by the responsible member of the executive body, provided that implementation of the SPG is ensured. This requires *inter alia* that the member of the executive body has sufficient resources to perform another function. Any exercise of several functions going beyond this (subject to that of the contact person) by one person must be limited to those cases in which the size of the person subject to due diligence does not permit the separation of duties (e.g. sole proprietorships).

As outlined above, the person subject to due diligence is responsible for the selection of the internal functions and also bears the responsibility for ensuring that these persons have, in particular, sound knowledge and/or experience in Liechtenstein due diligence law. In addition, the duty to exercise due diligence must, in particular, take into account any conflicts of interest. For example, it is generally not helpful if an internal function is assigned to a sales area in the company and/or if a sales employee holds an internal function. In the organisational structure, a clear separation between the first (employees directly involved in the business

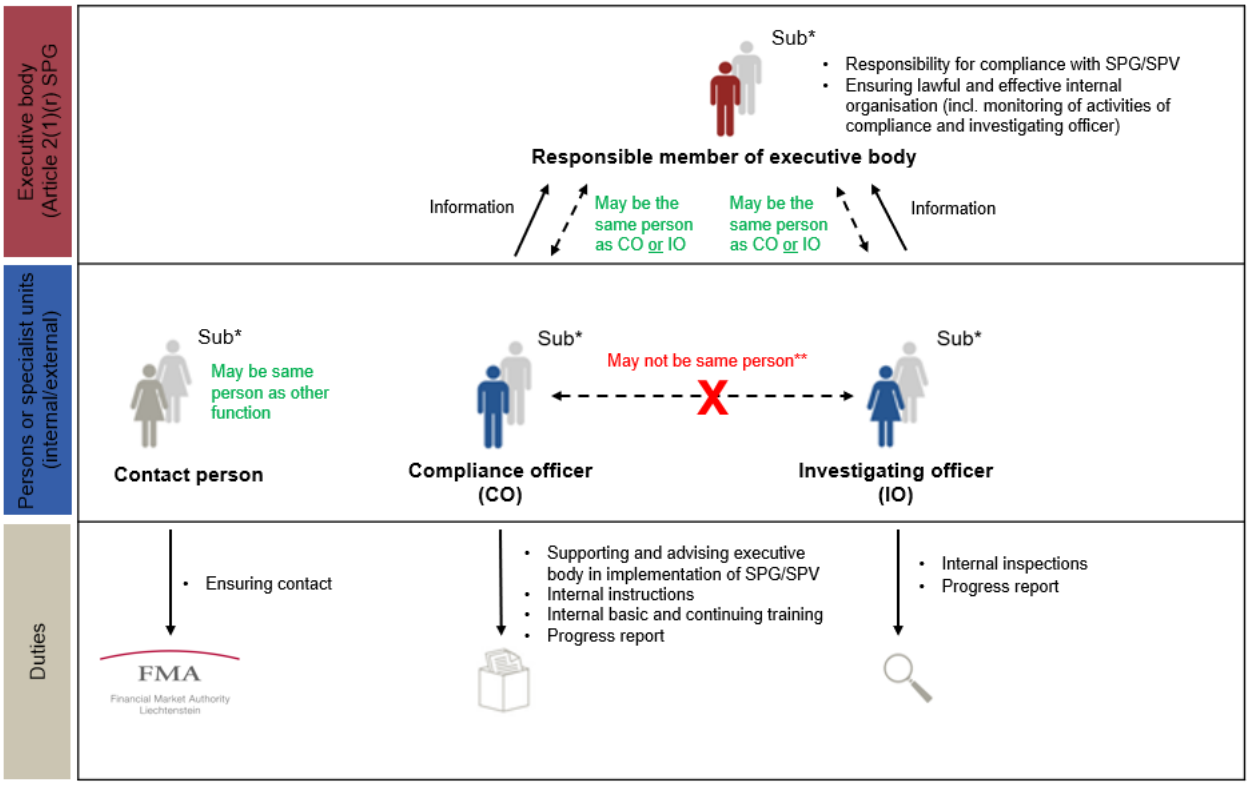
relationship), second (compliance officer and compliance) and third lines of defence (investigating officer and internal audit) must be ensured, insofar as this is possible in terms of size, and thus a clear division of tasks and independence within the company subject to due diligence must be guaranteed. This means, in particular, that the compliance officer only reports to the responsible member for SPG of the management level with regard to his or her tasks in terms of due diligence law and that the investigating officer can generally perform his or her tasks in terms of due diligence law free of directives. The inclusion of comprehensive rights to information, disclosure and inspection in the SPG directive forms the basis for structuring the organisation in accordance with the law.

As part of the fulfilment of his or her duties, the compliance officer shall submit a report to the entire management level detailing the activities of the past year. In addition to these activities, such a report also provides management with a summary of the current status of the implementations, the resources, the changes in risk, any backlog of activities to be carried out, new directive contents and an outlook on upcoming regulatory changes. Furthermore, the current company-wide risk assessment must also be communicated to the management level.

The investigating officer's report must contain an independent view of the status of the application and performance of all due diligence obligations and duties under the International Sanctions Act (ISA). In particular, the report must contain information on compliance with the reporting obligations, on any resource problems, and on the oversight of the second line of defence, as well as, in particular, a statement on the effectiveness of the system for combating money laundering and terrorist financing. The check and statement of the effectiveness of the system must be extended without restriction to all due diligence obligations.

If the duties of the compliance officer or investigating officer are delegated to appropriately qualified internal or external individuals or specialist units (delegation), the function holders remain responsible for the proper performance of their functions. The situation is only different if not only the duties, but also the function as such is transferred to a person or specialist unit. Substitution of internal functions must be guaranteed at all times. This means that for all the functions (contact person, compliance officer, investigating officer, responsible member of the executive body), a deputy must be appointed with the same required professional and hierarchical qualifications. With regard to the responsible member of the executive body, the appointment of a deputy may be waived in exceptional cases if, due to the size of the person subject to due diligence, no other qualified person is available (e.g. sole proprietorship). However, if the size of the person subject to due diligence permits, the person subject to due diligence must ensure that the required qualifications are fulfilled by an existing member of the executive body as deputy (e.g. through appropriate training). Notwithstanding this exception, however, in the event of a foreseeable extended period of absence (e.g. medical treatment, special leave), a new responsible member of the executive body within the meaning of due diligence law must be appointed for the duration of the absence. In such a case, it is sufficient for this person to have sufficient powers within the meaning of Article 36(2) SPV, but the appointment as a governing body of the legal entity is not mandatory.

To illustrate the above, please refer to the following illustration of internal functions:



* **Substitution**: Substitution of internal functions must be guaranteed at all times. (Exception: responsible member of executive body, if no other qualified person is available due to size of person subject to due diligence)
** **Exception**: Size of person subject to due diligence does not permit separation of duties

The FMA must be notified of the appointment and any change of function holders within five working days at the latest after the function has been taken up. The obligation to appoint and notify the internal function holders and their deputies applies to all persons subject to due diligence as referred to in Article 3(1) SPG. Consequently, natural persons who perform activities subject to due diligence as referred to in Article 3(1) SPG must also appoint internal function holders and their deputies and notify the FMA of their appointment or change. This applies in principle regardless of whether these natural persons are employed or self-employed. In exceptional cases, however, in the case of employed persons, it is considered sufficient if the (initial) notification of the appointment of the internal functions is made in consolidated form by the employer. All persons subject to due diligence to be attributed to the employer must be listed in the comments on the form provided for this purpose. If there is a subsequent change of employer in the case of employed persons, this does not trigger any obligation to notify. In that case, the FMA assumes that the internal function holders notified for the new employer also apply to the new employee, unless the FMA is actively notified otherwise.

The following form must be used for this notification: Form for the notification of the contact person, the compliance officer, the investigating officer, and/or the responsible member of the executive body.

The form must be signed by the internal function holders and evidence of in-depth expertise must be enclosed. Such evidence can be certificates of at least three days of specialised training at home or abroad[12] or the acquisition of such expertise by holding a comparable position at home or abroad for at least one year (full-time equivalent).

[12] Insofar as training abroad is involved, care must always be taken to ensure that the function holder also has adequate knowledge with regard to the special features of Liechtenstein due diligence law.

In order to meet the requirement of up-to-date knowledge, proof of attendance at a one-day specialist event per year is generally sufficient.

12. Transitional provisions in the SPG/SPV

With respect to the SPG and SPV amendments effective 1 September 2017, there are extensive transitional provisions to give the persons subject to due diligence sufficient time to implement the new obligations.

In general, the new law applies to business relationships existing at the time the SPG entered into force (1 September 2017) only as of 1 June 2018. This general rule is subject to the rules contained in paragraphs 7 and 8 of the transitional provisions on determining the beneficial owners of existing business relationships in accordance with the new definition of beneficial ownership. For existing business relationships to which simplified due diligence could be applied in the past, the new due diligence obligations must be met by 31 December 2018 at the latest.

With regard to the other transitional provisions and the provisions on entry into force, see the Law amending the Due Diligence Act, LGBl. 2017 No. 161, and the Ordinance amending the Due Diligence Ordinance, LGBl. 2017 No. 215.

13. Due diligence inspections

The persons subject to due diligence obligations are audited at regular, risk-based intervals by auditors and auditing companies commissioned by the FMA for compliance with the SPG and the SPV as well as the guidelines and notices issued by the FMA (ordinary due diligence checks). In exceptional cases, the FMA may deviate from this specified audit frequency.

In cases of doubt that the due diligence requirements are being met or if circumstances exist that appear to endanger the reputation of the financial centre, the FMA may also conduct extraordinary inspections or order them to be conducted.

Further details on the content of due diligence inspections can be found in FMA Guideline 2013/2 on due diligence inspections by mandated due diligence auditors.

14. Annual electronic reporting under the SPG (Article 37b(1)(a) SPV)

The revised Due Diligence Act, which entered into force on 1 September 2017, created comprehensive, risk-based due diligence supervision. For this purpose, different factors must be reported annually to the FMA by all persons subject to due diligence. The report to the FMA must be made by the persons subject to due diligence through an electronic reporting system.

For more detailed information, please refer to FMA Communication 2017/3 on electronic reporting in accordance with due diligence law.

15. Exercising due diligence in the transfer of funds

Article 5(2)(B)(2) SPG stipulates that due diligence must also be exercised in the case of money transfers. Furthermore, Article 12 SPG states that the Regulation (EU) No. 2015/847, which is directly applicable, applies to transfers of funds. In addition, the Joint Guideline JC/GL/2017/16 of the European Supervisory Authorities (ESA)[13] sets out what the ESA considers to be appropriate supervisory practices within the European system of financial supervision or how Union law should be applied in a particular area. According to Article 16(3) ESA Regulations[14], the competent authorities and persons subject to due diligence must make all necessary efforts to comply with the guidelines.

[13] Joint guidelines according to Article 25 of Regulation (EU) No. 2015/847 on the measures to be taken by payment service providers to identify the absence or incompleteness of information on the principal and the beneficiary and on the recommended procedures for processing a transfer of funds where the required information is missing (last amended on: 16.01.2018).
[14] Regulation (EU) No. 1093/2010; Regulation (EU) No. 1094/2010, Regulation (EU) No. 1095/2010.

16. Special obligations for persons subject to due diligence who are part of a group

Financial institutions subject to due diligence and TT service providers that are part of a group as defined in Article 2(1)(s) SPG must comply with the requirements for the global application of due diligence obligations. These take effect when several parts of the group are subject to due diligence. The obligations differ depending on whether the parent company is domiciled in Liechtenstein or not.

1. Parent company domiciled in Liechtenstein

If the parent company is domiciled in Liechtenstein, the responsibility for the global application of the due diligence obligations must generally rest with this person subject to due diligence. The essence of these obligations is a consistent approach to due diligence that extends across all obligated parties in the group. This is to avoid regulatory or supervisory arbitrage within the group. In order to achieve this objective, a second line of defence (comparable to the internal function of the compliance officer) as well as a third line of defence (comparable to the internal function of the investigating officer) must be established at the group. Above all, the responsibility for the global application must also be located at the management level (comparable to the internal function of the member responsible for the SPG at the management level). A first line of defence does not need to be installed at the group level, especially since the first line of defence of the respective group entities is responsible for ensuring compliance with group-wide strategies and procedures. While the third line of defence, together with the external auditors, is responsible for monitoring compliance with due diligence obligations in accordance with the law, including reporting to the management level, the second line of defence is responsible for the following tasks, among others. The second line of defence is committed to a uniform system of directives that specify the minimum standards under Liechtenstein law, to uniform standards and the facilitation of a basis for the exchange of information as well as to the guarantee of confidentiality of data, processing in conformity with data protection law and the observance of a group-wide ban on information (tipping off), to a regular exchange within the group at the level of the second line of defence, to the regular collection of reports from the respective entities as well as consolidated reporting to the management level, to the collection of risk data from the respective entities and the preparation of the group-wide risk analysis, the implementation of the group-wide measures to reduce the risk based on this, as well as to uniform standards and implementation of training and development for all relevant employees within the entire group.
The uniform system of directives (group-wide procedures and policies) must address and specify all of the aforementioned contents.

For the exchange of information, a regular fixed meeting of the second line of defence at the group level and of all obligated entities is a useful approach. The fixed meeting should at least discuss new regulations, sanctions lists, typologies and the measures to be derived from them. Other persons of the group entities who are to participate in the exchange of information (e.g. employees of the first line of defence) may be consulted.
Furthermore, the effects that international cases or suspicious activity reports in the individual entities have on the group should also be discussed. In particular, the focus is on effects on other entities within the group. In this context, reference is made to the tipping-off prohibition according to Article 18b SPG and the exception contained in Paragraph 3. If personal data is to be exchanged within the group, appropriate principles must be developed in advance in order to adequately protect the data subjects' rights. If the second or third line of defence at the group level cannot obtain relevant information from the entities because, for example, national law conflicts with the legal requirements for the global application of due diligence, the FMA must be informed in any case according to Article 16(3) SPG. The FMA also points out that the European Commission has issued a directly applicable regulation on the Anti-Money Laundering Directive by way of Delegated Regulation (EC) 2019/758. The Delegated Regulation provides further requirements on exchanges within the group and the associated obligations and measures.

2. Entity subject to due diligence domiciled in Liechtenstein

An entity domiciled in Liechtenstein that is subject to due diligence is obligated to provide the parent institution with all information that the latter requires in order to fulfil its group obligations concerning due diligence. If the group directive specifies minimum standards that do not correspond to the level of Liechtenstein due diligence law, the Liechtenstein due diligence standards must be met in addition to the obligations contained in the group directive. If personal data is transmitted in the context of the exchange of information, such data may only be transmitted if either a decision has been taken in accordance with Article 45(3) of the General Data Protection Regulation (GDPR) or if appropriate safeguards have been put in place in accordance with Article 46 GDPR so that the rights of the data subjects are protected.

17. Special obligations of persons subject to due diligence in respect of international sanctions

Liechtenstein has created the International Sanctions Act (ISA) for the domestic enforcement of international sanctions. The law authorises the government to take enforcement measures for the purpose of coercing international sanctions adopted by the United Nations (UN) or by the Principality of Liechtenstein's most important trading partners (e.g. European Union, Switzerland), which serve to ensure compliance with international law, in particular respect for human rights.

All currently valid enforcement measures are available at the following link: www.gesetze.li/konso/gebietssystematik?lrstart=946

The ISA is the central basis for Liechtenstein to implement international sanctions in the field of combating terrorism and terrorist financing. FATF Recommendation 6 also calls for the implementation of the relevant United Nations (UN) Security Council resolutions[15]. At this time, the following sanctions regulations are relevant in this context:

- Ordinance of 4 October 2011 on Measures concerning Persons and Organisations with Connections to the Taliban
- Ordinance of 4 October 2011 on Measures concerning Persons and Organisations with Connections to the Groups "ISIL (Daesh)" and "Al-Qaeda"
- Ordinance of 16 June 2020 on Measures against Certain Persons and Organisations to Fight Terrorism

Furthermore, the ISA serves as a basis for the implementation of international sanctions in the field of combating the proliferation of weapons of mass destruction (WMD) and their financing. FATF Recommendation 7 also calls for the implementation of the relevant UN Security Council resolutions.[16] At this time, the following sanctions regulations are relevant in this context:

- Ordinance of 24 May 2016 on Measures concerning the Democratic People's Republic of Korea

[15] According to FATF Recommendation 6, countries are expected to provide for targeted financial sanctions to comply with UN Security Council resolutions on preventing and combating terrorism and terrorist financing. The resolutions require countries to immediately freeze the funds or other assets of individuals or entities designated either (i) by or under the authority of the UN Security Council pursuant to Chapter VII of the Charter of the United Nations, including under Resolution 1267 (1999) and its successor resolutions; or (ii) by the respective country pursuant to Resolution 1373 (2001), and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of such persons or entities.

[16] According to FATF Recommendation 7, countries are expected to impose targeted financial sanctions to comply with UN Security Council resolutions to prevent, combat and disrupt the proliferation of weapons of mass destruction and their financing. These resolutions require countries to immediately freeze the funds or other assets of individuals or entities designated by or under the authority of the UN Security Council according to Chapter VII of the Charter of the United Nations and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of such persons or entities.

- Ordinance of 19 January 2016 on Measures concerning the Islamic Republic of Iran

The government must designate a competent enforcement authority in the enforcement measures imposed by ordinance in each case. This varies depending on the enforcement measures issued. Regarding financial sanctions, the Stabsstelle FIU is regularly designated as the competent enforcement authority. Since the most recent revision of the ISA (LGBl. 2020 No.13), the Financial Market Authority Liechtenstein (FMA) and the Liechtenstein Chamber of Lawyers (RAK) have been designated as supervisory authorities for compliance with the ISA obligations by persons subject to due diligence as defined in the SPG. This supervision concerns the special obligations according to Article 2c ISA for persons subject to due diligence under the Due Diligence Act. Based on the authorisation according to Article 5b(1)(a) ISA to issue a guidance, these special obligations are explained in the following Sections 17.1 and 17.2.

Detailed explanations on the subject matter of the ISA, on enforcement, on data and legal protection, on the punitive provisions as well as on applications for exemptions can be found in the ISA Guideline of the SFIU.[17] The SFIU's ISA Guideline contains, in particular, explanations on the reporting obligation concerning frozen funds and economic resources. These explanations concern the recognition of personal and non-cash benefits, the origin of the reporting obligation, the scope of the report as well as the technical reporting.

17.1 Obligation to verify ("screening")

According to Article 2c(1)(a) ISA, persons subject to due diligence shall verify client- and transaction-related documents to ensure compliance with the ISA and the relevant ordinances with respect to capital and payment transactions (this also includes transfers in tokens or virtual currencies).

Accordingly, persons subject to due diligence must verify compliance with the measures adopted to enforce international sanctions (sanctions lists), in particular with regard to the contracting partner (including authorised signatories or authorised representatives), the beneficial owner, the effective depositor, the recipient of distributions from discretionary legal entities, the beneficiary of life insurance policies and other insurance policies with an investment purpose, the business profile and with regard to transactions (see Article 2c(1)(a) ISA).

A verification in the above sense must first be carried out when entering into a new business relationship or carrying out an occasional transaction in order to ensure that the business relationship or the performance of the transaction is permissible and does not already violate sanctions (in particular, asset freezes or prohibitions regarding the provision of aid or resources). If, in the course of the business relationship, there are changes in the aforementioned persons (e.g. addition of new authorised signatories or authorised representatives), these persons must be verified immediately.

A verification must also be carried out immediately after the adoption or amendment of an enforcement measure. In each case, the entire client base must be verified with regard to the aforementioned personal roles.

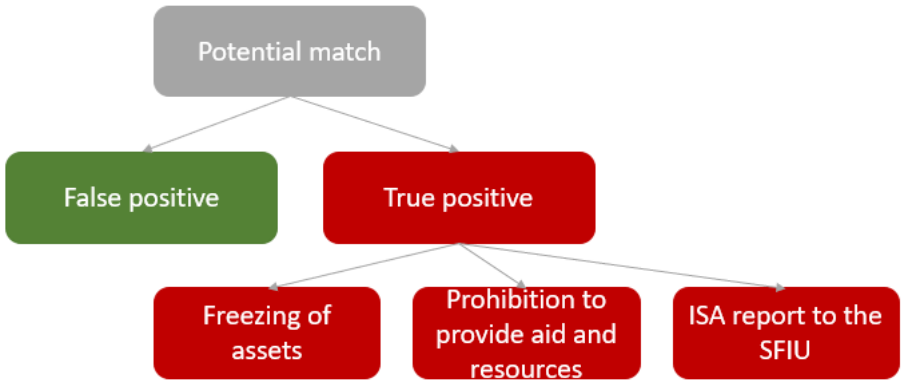
In addition, payment service providers in cross-border payment transactions must compare at least the following fields against the relevant current sanctions lists by means of real-time screening: payee (beneficiary), payment service provider of the payee, payer (principal), payment service provider of the payer (principal) and purpose of use (e.g. by means of a keyword search). The fields that are already checked within the framework of the continuous screening of the client base can be excluded.

Any sanction measures must also be verified in the case of investment services. This concerns both compliance with sanctions affecting the capital market and/or certain financial instruments (e.g. securities or money market instruments) as well as any custody accounts of sanctioned persons/entities.

[17] https://www.llv.li/inhalt/118924/amtsstellen/internationale-und-eu-sanktionen

As explained above, all persons subject to due diligence must carry out the verifications specified above in order to identify possible matches to the sanctions lists specified in the ISA ordinances. Sanctions lists contain a range of information that facilitates the identification of designated individuals or legal entities. In the case of individuals, this includes, for example, names, aliases, date of birth, nationality, identity card or passport information and/or last known address. For entities (legal entities, groups, companies or organisations), the sanctions lists usually contain name(s), aliases, address of registration, address of branch offices or other information.

Since certain names are very common, "potential matches" may frequently occur. However, this does not necessarily mean that the individual or legal entity, group, company or organisation with which the person subject to due diligence is dealing is in fact a designated person.



A person subject to due diligence who has identified a potential match shall suspend any transaction. The person subject to due diligence shall promptly verify whether or not the relevant person is a designated person or entity, taking into account the information obtained about the contracting partner (including authorised signatories or authorised representatives), the beneficial owner or the transaction in the course of due diligence or otherwise.

Only if the person subject to due diligence is convinced that the person or entity with a potential match is not a designated person or entity (false match; "false positive") will no action need to be taken, and the person subject to due diligence may then proceed with any suspended transaction. Persons subject to due diligence shall keep records of the measures described above so that they enable competent third parties to make a reliable judgement on compliance with the provisions of the ISA and the relevant ordinance.

However, if it cannot be ruled out that the potential match is a designated person or entity, or if the match is, in fact, clearly evident, this constitutes a true match ("true positive"). In this case, the person subject to due diligence shall immediately freeze the funds and economic resources concerned and ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of such persons or entities.[18]

It is further noted that persons and institutions holding or managing funds or knowing of economic resources that may be presumed to be covered by the freezing of an ISA ordinance shall report this to the Stabsstelle FIU immediately. As emphasised in the SFIU's ISA Guideline, a possible filing of a suspicious activity report according to Article 17(1) SPG does not exempt from the obligation to file an ISA report.

Additional information regarding screening

It is known that sanctioned parties provide and/or use false personal data in order to remain undetected in the sanction screening conducted by persons subject to due diligence. Furthermore, the data and information

[18] Insofar as this is provided for in the relevant ISA ordinance.

available to the person subject to due diligence may not exactly match the information in the sanctions lists. To maximise the effectiveness of screening, persons with due diligence should include variables such as:

- Different spellings of names;
- Name reversal (first/second names written as last names and vice versa);
- Abbreviated names (e.g. Will instead of William);
- Maiden names;
- Removal of numbers from entities; and
- Insertion/removal of points and spaces.

When using automated screening, the following measures help to improve screening quality:

- Understanding the capabilities and limitations of the respective automated screening system;
- Ensuring that the system is calibrated to the needs of the particular person subject to due diligence;
- Ensuring that the screening criteria have been set in proportion to the nature and size and ML/TF risk profile of the company to ensure that fewer "false matches" ("false positives") are produced;
- Risk-based use of fuzzy matching[19];
- Regular verifying of calibration and automated systems to ensure that they meet their purpose.

17.2 Organisational measures and appropriate internal inspection and monitoring measures

According to Article 2c(1)(b) ISA, persons subject to due diligence are required to take the necessary organisational measures and to ensure appropriate internal inspection and monitoring measures.

17.2.1 Responsibilities

In order to effectively comply with financial sanctions, the first step is to clearly define and align processes and associated tasks, competencies, checks, responsibilities, escalation levels when dealing with potential matches, as well as communication channels.

17.2.2 Internal directives

The person subject to due diligence shall ensure that business activities are conducted on the basis of organisational guidelines. To ensure compliance with financial sanctions, written work instructions or workflow descriptions must be in place for the individual operational areas (such as payment transactions, client registration) and for the compliance function. The appropriate level of detail of the organisational guidelines depends on the type, scope, complexity and risk content of the business activities.

The written work instructions must be made known to the employees concerned in an appropriate manner. These must be available to the employees in the respective current version. The work instructions must be adapted promptly in the event of changes in activities and processes.

17.2.3 Internal organisation

For each business area of the company, it is necessary to ensure that the aforementioned work instructions for compliance with financial sanctions are observed. Appropriate checks on business processes must be put in place for this purpose. This must be ensured by organisational means.

The internal organisation must be geared to the risk profile of the person subject to due diligence with regard to international financial sanctions and must be designed according to the type and size of the company as well as the number, type and complexity of the business relationships. The effective performance of internal functions as well as due diligence must be ensured at all times. In particular, persons subject to due diligence must ensure that they provide sufficient and appropriate human and technical resources to be able to comply with the obligations under the ISA and the relevant ordinances. The FMA also considers the contact person

[19] Fuzzy matching searches for words or names that are likely to be relevant, even if words, letters or spellings do not match exactly.

according to the SPG to be the contact person with regard to ISA compliance, unless another person is explicitly named by the person subject to due diligence.

- Compliance function (second line of defence)

The Compliance function must work towards the implementation of effective international financial sanctions compliance procedures and checks and monitor these checks. The compliance function should support and advise the management level, in particular, with respect to the implementation of the basic legal regulations. Compliance officers are expected to report regularly to the management level on compliance with financial sanctions.

- Independent audit function (third line of defence)

The company's financial sanctions compliance activities and processes must be reviewed by the internal audit function or by an investigating officer at appropriate intervals.

17.2.4 IT systems

The persons subject to due diligence shall use IT-supported screening systems or other procedures geared to the business activities and the risk situation in order to be able to immediately block and/or freeze accounts, deposits and assets in the event of new listings and to be able to comply with existing prohibitions on the disposal and provision of funds, also with regard to payment transactions.

The IT systems must be tested before they are used for the first time and after significant changes have been made, and must be approved by the employees responsible for the subject matter as well as by the employees responsible for the technical aspects. In addition, the IT systems and methods must be validated on a regular basis in order to check their appropriateness and/or functionality.

17.2.5 Documentation

All inspections and processes in connection with financial sanctions must be documented so that they enable expert third parties to make a reliable judgement on compliance with the provisions of the ISA and the relevant regulation. The inspection and surveillance documents prepared, including those relating to the processing of potential matches (and the decision criteria applied in the process), must be systematically drawn up and kept in a manner that is comprehensible to expert third parties. The timeliness and completeness of record keeping must be ensured.

Persons subject to due diligence must document all cases where potential matches with persons or entities on sanctions lists have been identified. This also applies to the verifications or enquiries subsequently made, regardless of whether the match is ultimately a true positive or a false positive. In the case of genuine matches, the measures subsequently taken must be documented.

17.2.6 Training

Persons subject to due diligence must train relevant employees in international financial sanctions on a regular basis, i.e. at least once a year.

The training (internal or external) must cover, in particular, the internal procedures and processes involved in identifying sanctioned persons and entities, the handling of potential matches and the further handling of actual matches (freezing, prohibitions regarding the provision of aid and resources as well as reporting to the SFIU). The training must be conducted for first, second and third line of defence staff as well as for the management level.

18. Final provisions and transitional periods

The entire instruction, including the General and Special Part, applies effective 24 April 2018 and replaces all previous sector-specific instructions.

The amendments of 7 May 2019 entered into force on that day. For business relationships existing at the time of the entry into force of those amendments, the amendments in the **General Part, point 5.3**, which concern

- verification of the identity of the beneficial owner by means of risk-based and adequate measures (obtaining documents with probative value for the purpose of Article 7 SPV with the exception of cases of low risk), and

- verification of beneficial ownership in cases of normal risk by means of further measures such as obtaining or inspective appropriate documents

as well as the amendments in the **Special Part on service providers for legal entities, point 4.2**, which concern

- verification of the identity of the distribution recipient by appropriate measures (obtaining documents with probative value for the purpose of Article 7 SPV)

enter into effect on **7 May 2020**.

The amendments of 27 December 2019 concerning TT service providers subject to due diligence and other persons subject to due diligence with a nexus to TT services and virtual currencies and tokens enter into force on **1 January 2020**.

The amendments of 11 March 2020 enter into force on **15 April 2020**.

The changes of 25 August 2021 came into effect on the same day. For business relationships existing at the time these amendments come into force, the amendments in the **General Part, Section 6** that

- concern known related parties according to Article 2(3)(c) SPV (closely connected socially or politically)

apply from 31 August 2022 (see the transitional period SPV in effect on 1 September 2021).

The internal directives, **General Part, Section 11.2.1,** with regard to the design and implementation of inspection and monitoring measures for investigating officers; Article 31 (2)(g^{bis}) SPV in conjunction with Article 35 SPV must be amended by 30 June 2022 at the latest (see the transitional period SPV in effect on 1 September 2021).

Amendments to the **Special Part** for persons who trade in works of art or act as intermediaries in the trade in works of art (Article 3(1)(u) SPG) as well as persons who professionally hold assets belonging to third parties in safe custody as well as rent out premises for the safekeeping of valuables (Article 3(1)(v) SPG) will apply from 1 October 2021 (see the transitional period SPG in effect on 1 April 2021).

The amendments of 13 April 2022 enter into force on **15 April 2020**.

Updated: 13 April 2022

II. Special Part

Undertakings for collective investment (Article 3(1)(c) SPG)

1. Scope and application of due diligence obligations

1.1 General information

In the course of the adoption of the Anti-Money Laundering Directive (EU), the due diligence obligation was attached to undertakings for collective investment (UCIs).[20] All of the following statements apply to the undertaking for collective investment and – if applicable – to bodies of the investment company as well as to the manager (management company/AIFM) as the representative of the fund[21]. Self-managed investment companies act for themselves.

By way of introduction, it should be noted that the following describes the due diligence obligations from the perspective of the UCI subject to due diligence with regard to the business relationship with subscribing persons. The following explanations are not relevant for other persons subject to due diligence (e.g. depositary, asset manager, etc.) who have to apply due diligence obligations in relation to a business relationship with a UCI.

Insofar as the simplifications explained in the following Section 1.2 are not applicable when determining the contracting partner and the beneficial owner in the case of business relationships of the fund according to Article 22b(3) SPV[22]:

- the contracting partner must be identified properly according to Article 6(1) SPG;
- when determining and verifying the identity of the beneficial owner, it must be determined for which third party account (and/or for which end client) the subscribing institution is acting. Such person(s) are then deemed to be the beneficial owner(s) of the business relationship. If the subscribing institution acts on behalf of one or more individuals, a written declaration for individuals must be issued (there is no standard form for this). If the subscribing institution acts on behalf of an entity according to Article 3(1)(a) SPV (corporation or entity similar to a corporation), Form C may be used, in which case it must be made clear that it is not the circumstances of the subscribing institution that are reflected, but rather the circumstances of the legal entity for which the subscribing institution has acquired the fund units. If the subscribing institution acts on behalf of a legal entity according to Article 3(1)(b) SPV (foundation, trust or similar legal entity), Form T may be used for this purpose. Here, too, it must be clarified that not the circumstances of the subscribing institution but the circumstances of the legal entity for which the subscribing institution has acquired the fund units are reflected; and
- any change to the beneficial ownership in the fund must be documented immediately and the relevant forms must be amended accordingly.

1.2 Simplified application of due diligence obligations

Article 22b(3) SPV provides that in the case of unit subscriptions of undertakings for collective investment in transferable securities (UCITS) or alternative investment funds (AIFs) by institutions domiciled in an EEA

[20] Undertakings for collective investment have been subject to due diligence since 1 September 2017. A transitional provision stipulates that the new law applies from 1 April 2018 to persons subject to due diligence according to Article 3(1)(c) SPG who were exempt from the scope of the Due Diligence Act under the previous law (i.e. maintenance of the share register not by the management company/AIFM but by the depositaries).

[21] Fund means any sub-fund of an umbrella fund or a single fund.

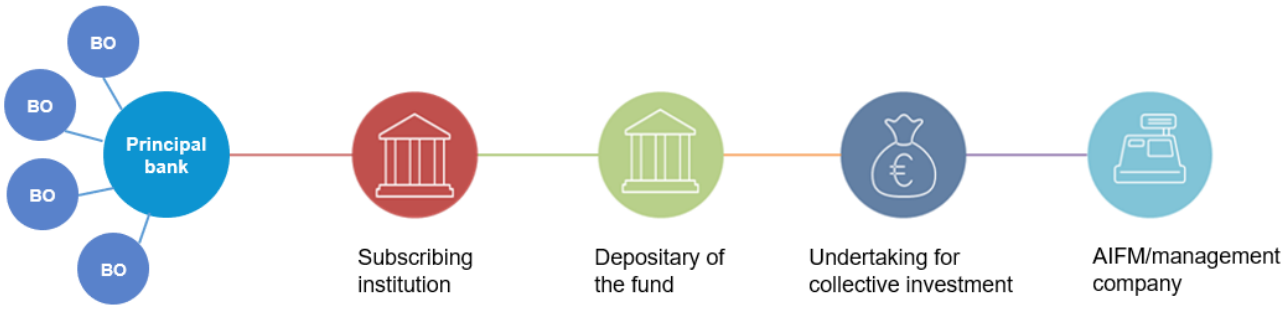
[22] This also applies in the event that a third country previously listed in Annex 1 no longer meets the equivalence criteria and is consequently no longer listed in Annex 1 (e.g. due to a reassessment by the FATF). Article 22b(3) SPV may subsequently no longer be applied to new business relationships and/or new fund subscriptions. However, this amendment does not lead to a situation where past fund subscriptions by institutions from the third country in question have to be processed.

member state or an equivalent country within the meaning of Chapter IV Annex 1 of these Guidelines[23], the obligation to determine the contracting partner and the beneficial owner may be met by the UCI subject to due diligence by:

a) establishing the identity of the subscribing institution by means of a share register or a subscription form;

b) taking risk-based measures to ensure that the risk in relation to money laundering, organised crime and terrorist financing is low based on the assessment of client, product, investment, distribution channel and country risks; and

c) checking the subscribing institution's internal inspection and monitoring measures in order to ensure that the subscribing institution exercises risk-based and appropriate due diligence with its own clients within the meaning of Article 5(1) of the Act.



Check of client, product, investment, distribution channel and country risks (Letter b)

Central to this are the measures to be taken in accordance with Letter b. The assessment of client, product, investment, distribution channel and country risks must be carried out on the basis of the criteria in Section 2.

As a matter of law, the simplifications of Article 22b(3) SPV must not be applied to:

- UCIs which do not comply with the requirements of Directive 2011/61/EU or Directive 2009/65/EC:
  - Investment companies under the Investment Undertakings Act (IUA; *Investmentunternehmensgesetz* – IUG)
  - AIF and AIFM and/or UCITS and management company are not domiciled and established in the EU/EEA and the fund is not authorised for marketing in the EU/EEA
- Subscriptions from institutions from a non-equivalent third country and/or high-risk country (cf. Annex 4 SPV)
  - UCIs that are used for individual asset structuring.[24]

The prohibition of the application of Article 22b(3) SPV in connection with UCIs used for individual asset structuring is based on the explanations in Chapter 9 of the Risk Factor Guidelines of the European Banking Authority ("EBA Guidelines on ML/TF risk factors"). Accordingly, the risk of abuse for ML/TF purposes is inherently higher for UCIs intended for a limited number of wealthy individuals or families than for mutual funds, because in this case it is more likely that investors hold a position that allows them to control the fund's capital. Funds whose capital is controlled by investors are considered as instruments for individual asset structuring according to the ESA Risk Factor Guidelines and are designated as risk-increasing factors in Annex III of Directive (EU) 2015/849. Internationally, such funds are also referred to as "private placement funds".

[23] The compliance check with the requirements according to Article 22b(3) SPV (including the domicile and supervision in an equivalent country) must be proven upon request of the FMA.
[24] Wording according to Annex III of the Anti-Money Laundering Directive (EU) 2015/849: "legal persons or arrangements that are personal asset-holding vehicles".

In order to assess whether a UCI in the above sense exists, the persons subject to due diligence shall examine the documents submitted and prepared in connection with the establishment of the fund and shall ask the parties involved in the fund business, such as the depositary, the fund promoter, the subscribing institution or also the investor himself or herself – to the extent that he or she is known – whether there is any information or indication that the fund is intended to serve only a small circle of investors or as a mutual fund for a broadly diversified group of investors.

These clarifications must be carried out on the basis of risk and documented accordingly. The fund subject to due diligence cannot be held responsible if information on the group of investors is intentionally concealed within the scope of these enquiries; however, the fund subject to due diligence must check the plausibility of the statements to the best of its ability.

In particular, the following information must be investigated in connection with the clarification:

- The UCI has knowledge that an investor holds and/or will hold more than 25% of the units;[25]
- there is evidence in the documents submitted for the establishment of the fund that the fund is being established for the interest of certain persons;
- the UCI is only open to a very limited group of investors;
- performance review with specific persons (groups);
- there is no trading in units over a longer period of time, and it is not a closed-end UCI;
- q relevant part of the fund units is issued on the basis of contributions in kind.

This information must be clarified, for example, by questioning the parties involved in the fund transaction, such as the depositary, the fund promoter, the subscribing institution or the investor himself or herself. The existence of a single indication does not necessarily mean that the UCI must be categorised as a UCI for individual asset structuring. This involves circumstantial evidence of varying significance. The clarification of the information and the consideration of all circumstances of the fund are decisive in order to be able to make a final assessment as to whether the UCI may be used for individual asset structuring or not. For example, it may be that only one institutional investor invests in the fund, but this investor bundles the interests of numerous investors, which means that the UCI is not used for individual asset structuring. It is also conceivable that a fund offers performance reviews for investors due to special events – even if the fund has a broad range of investors. Furthermore, seed capital could also be used to finance innovation in the form of a fund in order to open it up to the general public if the fund enjoys a certain level of success. These examples show that the UCI must investigate and clarify information on individual asset structuring. However, even if such information is available, there is no compelling reason to assume the existence of a UCI for the purpose of individual asset structuring.

Similarly, a UCI is generally not to be assumed to be used for individual asset structuring if an asset manager wants to continue an investment strategy for a large number of clients by means of a fund and all the assets of the existing investment accounts are brought into the fund. The situation is different, however, if only the custody accounts of a small number of clients with whom there are, for example, performance discussions concerning the fund are brought into a fund.

On the other hand, there may also be information indicating the existence of a mutual fund or generally the admissibility of the application of Article 22b(3) SPV, in particular if:

- the investor in the fund is a state pension fund or a company pension scheme;
- a low minimum investment is specified in the fund prospectus;[26]
- funds that are not authorised for distribution to third parties, but serve the internal implementation of a uniform investment strategy for several clients.

<u>Check of the internal control and monitoring measures of the subscribing institution (Letter c)</u>

[25] The 25% threshold should not be taken into account in the formation or liquidation phase of the fund. The formation phase of the fund may generally last 12 months from the date of payment.
[26] By way of clarification, it should be noted that the existence of such information alone does not automatically mean that a broad range of investors can be assumed. It is only one piece of evidence, which must be considered and assessed together with the other information.

In addition to determining the identity of the subscribing institution on the basis of a share register or a subscription certificate (Letter a) and checking the client, product, investment, distribution channel and country risks (Letter b), the internal control and monitoring measures of the subscribing institution must be checked (Letter c).

For a verification of the internal control and monitoring measures of the subscribing institution, the inspection of the register of holders of licences at the competent supervisory authority is in any case not sufficient. Instead, a concrete verification is required. This can take the form of targeted due diligence questionnaires, for example, as well as risk-based screening for negative media reports and international sanctions. Any matches in the course of media coverage must be assessed for their relevance and potential impact on the person subject to due diligence. An on-site check of the control and monitoring measures at the subscribing institution is not mandatory.

The duties under Letter c may be delegated or outsourced to the depositaries, with the responsibility remaining with the person subject to due diligence.

The compliance check with the requirements according to Article 22b(3) SPV (including the domicile and supervision of the subscribing institution in an equivalent country) must be proven upon request of the FMA. If the conditions according to Article 22b(3) SPV are met, the UCI must therefore record the subscribing institution in order to determine the contracting partner and the beneficial owner (no formal determination necessary).

A minimum of monitoring of the business relationship must always remain in place in order to be able to guarantee the obligation to notify the SFIU in accordance with Article 17 SPG. Minimum supervision means that, despite the application of simplified due diligence, attention must be paid to the normal conduct of the business relationship in terms of due diligence. In other words, the conduct of normal business activities constitutes the basis for a possible suspicious activity report. In the normal course of business, regular sanctions and media screening as well as regular screening of investments with regard to ML/TF risks and any clarifications of the results must be performed. No further activity beyond normal business activities is required. Based on this, the person subject to due diligence knows the subscriber and/or the subscribing institution, the fund promoter as well as the investment and is therefore generally in a position to recognise and report any anomalies and deviations from normal business behaviour.

2. Risk assessment

The risk assessment must be performed, on the one hand, at the level of the person subject to due diligence (sub-fund/single fund) and, on the other hand, at the level of the business relationship. In accordance with the legal requirements, this must be done at and/or before the start of the business relationship. With regard to funds that are subject to Article 22b(3) SPV, a risk assessment of new business relationships must be done in this regard during the monthly reconciliation with the share register.

Since the risk assessment at the level of the person subject to due diligence (sub-fund/single fund) has a decisive impact on the final application of the due diligence obligations, this must therefore be carried out before a business relationship is entered into.

In addition to information on the investor group (business relationships), the risk assessment of the fund also takes into account the money laundering and terrorist financing risk of the distribution channel, that is, in particular, the fund promoter[27], as well as the investment in accordance with Article 22a(1bis) SPV. Any new business relationships that are entered into must also be subjected to a risk assessment. If the business relationship increases the risk for the fund, the risk assessment of the fund must also be updated immediately.

In connection with the investment, investments in sensitive sectors or high-risk countries, in particular, must be considered risk-increasing factors in accordance with Annex 4 SPV. An investment in listed securities (including hedging instruments) has a risk-reducing effect. With regard to the investment, it must be made

[27] The fund promoter is relevant for the distribution channel risk if the promoter also has a link to the (potential) group of investors.

clear that any prudential risk (e.g. lack of diversification of the portfolio) does not necessarily represent a money laundering and terrorist financing risk. For example, from the point of view of client protection, an investment in a single blue chip stock usually represents a portfolio that is not diversified enough and thus carries an increased investor risk. From a money laundering and terrorist financing risk perspective, blue chip stocks are exchange-traded securities that mitigate ML/TF risk.

In connection with the group of investors, depending on the structure of the distribution of the UCI, it is sometimes not possible to factor in the risks with regard to the beneficial owners, since only the subscribing institutions are known. In these cases, the risks must be assessed with regard to the subscribing institution. Subscribing institutions outside the EEA and equivalent third countries according to Annex 1 are indicative of a high risk, which directly precludes the application of simplified due diligence requirements. Furthermore, it is also considered a high risk which directly precludes the application of simplified due diligence obligations if the fund promoter comes from a high-risk country according to Article 4 SPV or if the UCI is used for individual asset structuring. The specific risks of the group of investors must be included in the risk assessment of the fund where the group of investors is known (if Article 22b(3) SPV does not apply). Clarifications in this regard must be documented in the due diligence file.

In connection with the distribution channel risk, the risk emanating from the fund promoter, in particular, must be factored into the risk assessment. The fund promoter is relevant for the distribution channel risk if the promoter also has a link to the (potential) group of investors. In this context, the geographical environment as well as any information from the sanction and media screening of the fund promoter must be included in the risk assessment. The application of simplified due diligence obligations is therefore excluded if the fund promoter is domiciled in a high-risk country according to Annex 4 SPV. In these cases, special attention must be paid to the group of investors originating from the fund promoter's environment.

Whether a risk factor increases or decreases the ML/TF risk of the fund depends on the consideration of the risk factor in the overall context. For example, a contribution in kind need not in itself give rise to an increased risk. However, if it is a contribution in kind that does not make sense in the overall context of the fund or if it is structured in such a way that it is only likely to be of interest to a small group of investors who are connected to this contribution in kind, then this contribution in kind constitutes a risk-increasing element. It is therefore fundamental that risk-increasing and risk-reducing factors be clarified to the extent that their impact can be assessed in the overall context of the fund.

Examples of risk factors that affect the risk assessment are listed below:

2.1 Risk-mitigating factors

Risk factors with low risk:

- Listed fund

Risk-mitigating factors:

- Investment in listed securities[28]
- Mutual funds with a large number of investors (widely distributed)
- Subscribing institution in EEA/equivalent third country

2.2 Risk-increasing factors

Risk factors with high risk:

- Subscribing institution outside EEA/equivalent third country
- Fund promoter from a high-risk country

[28] As a rule, investments in listed securities mitigate risk. However, if the group of investors is known, attention must always be paid to any possible connection of the investors to the investments themselves (risk: insider trading).

- UCI is used for individual asset structuring

Risk-increasing factors:

- Contributions in kind
- Additional layer for insurance policies
- Fund promoter from at-risk countries
- Non-listed investments in sensitive sectors (raw materials, etc.)
- Complex investment structures
- Non-listed investments in at-risk countries
- Complex structures regarding the business relationships of the fund[29]
- PEPs in connection with the business relationships of the fund[30]
- Connection to high-risk country(ies) of the contracting partner or the beneficial owner(s) regarding business relationships of the fund

2.3 Risk-based approach

The person subject to due diligence shall generally classify the business relationships according to a risk-based approach on an individual basis. Criteria eligible for business relationships and transactions with increased risks are listed in the ESA Risk Factor Guidelines, in Article 11 SPG and in Annex II SPG. However, these are not exhaustive. This means that the person subject to due diligence, with reference to Article 9a SPG, shall define his or her own criteria in addition to the cases regulated by law, insofar as this appears necessary due to special circumstances. The applicability of the enhanced due diligence obligations can thus result both from the legal factors (cf. Article 11(3) to (6) SPG) and from the risk classification according to Article 9a SPG.
Where there are risk factors that require the application of regular or enhanced due diligence, the simplifications according to Article 22b(3) SPV cannot be applied.
If it is determined on the basis of the existence of a high risk or on the basis of the risk assessment carried out at the level of the fund that simplified due diligence obligations cannot be applied, this determination will be extended to the level of the business relationships. Consequently, no simplified due diligence must be applied to the fund's business relationships.

The higher the risk, the greater the effort in terms of clarification and obtaining information. Particularly with regard to the subscribing institution, the fund promoter and the end investors (beneficial owners of the fund's business relationships), the need for clarification increases as the risk increases.
The risk factors with low risk outlined above allow by themselves for the application of simplified due diligence. By contrast, the above risk factors with high risk preclude the application of simplified due diligence.

- Application to existing business relationships as of 1 September 2021

In the case of existing business relationships, a review must be done as part of the update of the business profile or risk assessment. Such review of the risk assessment must be performed by 31 December 2021 at the latest. The review of existing business relationships and the collection of further information, in particular on the end investor (insofar as Article 22b(3) SPV is not applicable), must be carried out in this respect by 31 December 2022.

- Application to newly established business relationships as of 31 December 2021

In the case of newly established business relationships in the period from 1 September 2021 to 31 December 2021, the obligations must be fulfilled by 31 December 2021 at the latest.

[29] With regard to the definition of complex structures, please refer to Section 5.2.3 of FMA Guideline 2013/1.
[30] PEPs in connection with the business relationships of the fund are only relevant in the application of Article 22b(3) to the extent that they are known to the person subject to due diligence.

3. Business profile

With regard to the periodicity of the obligation to update the business profile, reference is made to the explanations under Section 5.4.2 in the General Part. In the event of significant changes to the investment that increase the ML/TF risk, the business profile must be updated immediately.

In the event of the applicability of Article 22b(3) SPV, the business profile must in any case be updated monthly when a new subscribing entity is entered in the share register, although every business relationship must be recorded.

In practice, the depositary usually keeps the share register (on behalf of the management company/AIFM) so that the depositary has up-to-date information on new subscriptions and redemptions. The fund (and/or the management company/AIFM) must therefore ensure that this information is accessible.

4. Due diligence files

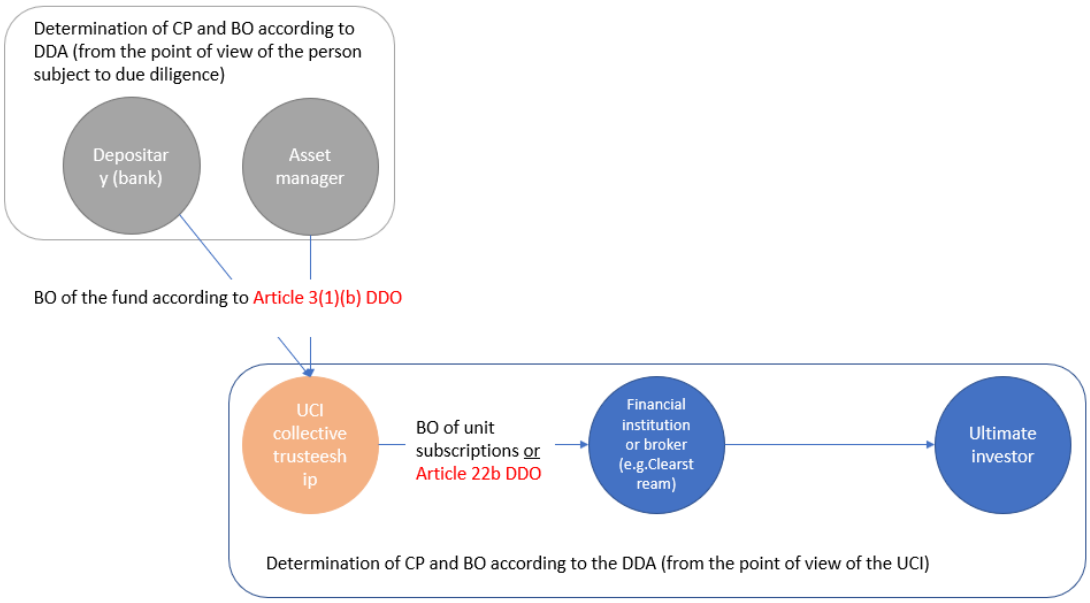
All risk assessment clarifications must be documented in the due diligence file. In the case of funds, this applies, in particular, to relevant information and clarifications (media research and others) on the fund promoter, which subsequently enable an independent third party to reproduce the results in the risk assessment. Where the fund promoter is a group company (e.g. parent company) or if the tasks of the fund promoter are performed by the management company or the fund itself, this must be noted in the due diligence file. In these cases, a determination as well as a related screening of the fund promoter can be waived.

A risk-based recording of the investment side with respect to the ML/TF risk must be made with regard to the investment. As such, it is not relevant which listed securities are invested in. It is only relevant that investments are made in listed securities. The more specific the investment, the more detailed the information should be. For example, in the case of contributions in kind, concrete information about these must be obtained and documented so that it is also verifiable in the context of the risk assessment check.

Furthermore, the relevant clarifications as to whether the fund is used for individual asset structuring must be documented in the due diligence file. In particular, information obtained from the fund promoter, the subscribing institution[31] and/or any direct contact with the investor as well as clarifications regarding further information must be documented.

Clarifications relating to the risk factors must be documented in such a way as to allow for subsequent risk assessment and traceability of the clarification.

[31] If no information is provided by subscribing institutions in the context of the risk assessment, this must be documented, stating the relevant reasons. It should be noted that this only applies in connection with the risk assessment and not in connection with the determination and verification of beneficial owners in the event of non-application of Article 22b(3) SPV.



Management companies with individual portfolio management (as additional service)

The Special Part contains guidance supplementary to the General Part for each sector. Both parts form an integral document and must therefore be read together.

Specific questions of interpretation can be discussed with the FMA.

The EU Anti-Money Laundering Directive applies to natural or legal persons acting in the exercise of their professional activities relating to the management of client money, securities or other assets (see Article 2(1)(3)(b)(ii) of Directive EU 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing). These rules have been implemented in Article 3(1)(i) SPG. Management companies for funds (UCITS and/or AIFs) with the additional licence for individual portfolio management are comparable to asset management companies with regard to this activity, so that the same due diligence obligations apply as for an asset management company as referred to in Article 3(1)(i) SPG.

Accordingly, all guidance applicable to asset managers also applies *mutatis mutandis* to management companies with individual portfolio management as an additional service in regard to their individual portfolio management.

Insurance undertakings (Article 3(1)(d) SPG)

1. Addressees/scope

Article 3(1)(d) SPG places insurance undertakings with a licence under the Insurance Supervision Act, insofar as they offer direct life insurance, under the SPG. Pursuant to Article 3(2) in conjunction with Article 3(1)(d) SPG, Liechtenstein branches of foreign insurance undertakings are also subject to the SPG insofar as they offer direct life insurance.

Due to their low risk of being abused for activities in connection with money laundering, organised crime, or terrorist financing, Article 4(a) SPG excludes institutions exclusively operating in the field of occupational old age, disability, and survivors' provision. These primarily include pension schemes under the Occupational Pensions Act (BPVG) and pension funds under the Pension Funds Act (PFG).

An analogous application of Article 4(a) SPG is appropriate for insurance products where benefits are provided exclusively for institutions for occupational provision under the BPVG and PFG that wish to cover their risks externally (reinsurance of death and disability risks of pension schemes). In this case, the death and disability risks for pension schemes and pension funds are insured in order to balance the risks that cannot be assumed by individual pension schemes and pension funds, in particular the insurance of increased individual risks and the reinsurance of extraordinary overall losses.

The same also applies if risk coverage is offered for pension schemes outside tax-privileged occupational pension provision. The precondition is that the contracting parties in these cases are also only pension schemes within the meaning of the BPVG. Contracts that are concluded not with pension schemes but with professional associations or other collectives that are not considered to be institutions for occupational provision within the meaning of Article 4(a) SPG accordingly fall within the scope of the SPG.

2. Due diligence obligations

2.1 Timing of exercising due diligence

All due diligence obligations under Article 5(1) SPG must in principle be performed by the insurance undertakings when the business relationship is established, i.e. when the application for the policy is submitted, but at the latest before the life insurance contract is definitively concluded.

Only in cases where this is necessary to maintain normal conduct of business and a low risk of money laundering and terrorist financing has been established under Article 10 SPG, the verification of the identity of the contracting party or the beneficial owner can be completed after the business relationship has been established. The verification must be carried out as soon as possible after the first contact and it must be ensured that no outflow of assets takes place in the meantime (Article 18(2) SPV).

2.2 Determination and verification of the contracting partner's identity (Article 6 SPG; Articles 6 et seq. SPV)

The insurance undertakings must as a rule identify and verify the policyholder of a life insurance contract as the contracting party for the purpose of Article 6 SPG. If doubts arise about the identity of the contracting party in the course of the business relationship, the identification and verification of the identity of the contracting party must be repeated.

If the policyholder of an existing insurance contract is replaced by a different policyholder – especially as a consequence of assignment – the contracting party and the beneficial owner must be identified and verified again. (Article 15(3) SPV)

2.3 Determination and verification of the identity of the beneficial owner and the beneficiary (Articles 7 and 7a SPG, Articles 11 et seq. SPV)

In the case of insurance contracts, the natural persons who ultimately pay the insurance premiums are deemed the beneficial owners. They must be identified and verified in accordance with the principle set out in Article 7 SPG.

Pursuant to Article 7b SPG, in the case of life insurance policies and other insurances taken out with an investment purpose, the insurance undertakings must establish the identity of the beneficiary at the time of paying out and take appropriate steps to verify that identity. The same principles apply to the determination and verification of the identity of the beneficiary as to the beneficial owner (see General Part, Section 5.3). If the beneficiary is a legal entity, the identity of its beneficial owners must be established and verified. The forms in Annex 1 SPV (Form C and/or T) must be used to determine such beneficial owner.

Already at the time when the contract is concluded, insurance undertakings must record the name of the beneficiaries identified as a natural person specified by a name or as a legal entity. For beneficiaries whose identity is established from characteristics or by category or in another way, they must obtain sufficient information in respect of these beneficiaries in order to ensure that they are able to establish their identity at the time of paying out.

3. Delegation

In principle, insurance undertakings may delegate the performance of due diligence obligations under Article 5(1)(a) to (c) SPG to certain third parties under the conditions of Article 14 SPG. In this context, they must ensure that the data and documents gathered by the third party under the SPG are immediately transmitted to them and that the delegate confirms by signature the conformity of the copies produced with the originals or authenticated copies. Even in the case of delegation, the responsibility for proper compliance with the due diligence obligations always remains with the delegating insurance undertaking. This responsibility also includes ensuring that there is no sub-delegation. This can be ensured, for example, by the delegation agreement providing for a prohibition of sub-delegation.

This means due diligence obligations may be delegated to registered master intermediaries (master pools or intermediary pools). Sub-delegation by the master intermediary, however, is excluded according to Article 24(3) SPV. If recourse is had to the insurance intermediaries affiliated with the master intermediary, the due diligence obligations must be delegated to them directly by the insurance undertaking, taking into account Article 14(1) SPG.

Insurance intermediaries (Article 3(1)(g) SPG)

1. Addressees/scope

Article 3(1)(g) SPG subordinates insurance brokers licensed under the Insurance Distribution Act to the SPG, insofar as they broker life insurance contracts and other investment-related services.

In principle, all activities relating to the distribution of life insurance policies are covered by the SPG, i.e. advising, proposing, or carrying out other preparatory work for their conclusion and assisting in the management or performance of contracts (portfolio management). The SPG also covers the provision of information on life insurance contracts based on criteria chosen by a client via a website or other media, and the establishment of a ranking of life insurance products, including a price and product comparison or a price discount if the client can conclude the life insurance contract directly or indirectly via the website or other media. The due diligence obligations to be performed relate to the insurance contract to be brokered and not to the brokerage contract.

According to Article 4(a) SPG, the mediation of affiliation contracts for institutions of occupational provision does not fall within the scope of the SPG *(see Special Part on insurance undertakings)*.

2. Due diligence obligations

All due diligence obligations under Article 5(1) SPG must in principle be performed by the insurance brokers when the business relationship is established, i.e. when the application for the policy is submitted, but at the latest before the life insurance contract is definitively concluded.

Only in cases where this is necessary to maintain normal conduct of business and a low risk of money laundering and terrorist financing has been established under Article 10 SPG, the verification of the identity of the contracting party or the beneficial owner can be completed after the business relationship has been established. The verification must be carried out as soon as possible after the first contact and, to the extent possible for the insurance broker, it must be ensured that no outflow of assets takes place in the meantime.

The insurance brokers must as a rule identify and verify the policyholder of a life insurance contract as the contracting party for the purpose of Article 6 SPG. If doubts arise about the identity of the contracting party in the course of the business relationship, the identification and verification of the identity of the contracting party must be repeated.

If the policyholder of an existing insurance contract is replaced by a different policyholder – especially as a consequence of assignment – the contracting party and the beneficial owner must be identified and verified again. (Article 15(3) SPV)

In the case of insurance contracts, the natural persons who ultimately pay the insurance premiums are deemed the beneficial owners. They must be identified and verified in accordance with the requirements set out in Article 7 SPG.

Under Article 9(1) SPG, insurance brokers must carry out timely risk-appropriate monitoring of their business relationships to ensure that they are consistent with the business profile (Article 8 SPG). This also includes monitoring the transactions performed in the course of the business relationship, insofar as it is possible for the insurance broker to do so.

The duty to monitor the business relationship is waived only if, after conclusion of the insurance contract between the policyholder and the insurance undertaking, the insurance broker has no access to information on the further course of the insurance contract and no further contact with the policyholder, or if the broker contract does not give rise to any responsibilities for the further support and advice of the policyholder or the handling of changes to the insurance contract.

3. Delegation

In principle, insurance brokers may delegate the performance of due diligence obligations under Article 5(1)(a) to (c) SPG to certain third parties under the conditions of Article 14 SPG. In this context, they must ensure that the data and documents gathered by the third party under the SPG are immediately transmitted to them and that the delegate confirms by signature the conformity of the copies produced with the originals or authenticated copies. Even in the case of delegation, the responsibility for proper compliance with the due diligence obligations always remains with the delegating insurance broker.

The relationship between insurance undertakings and insurance brokers regularly gives rise to a situation in which an insurance undertaking delegates the identification and verification of the identity of the contracting party and the beneficial owner or the creation of the business profile to the insurance broker. In such cases, insurance brokers then in principle assume the due diligence obligations on behalf of the insurance undertaking and at the same time on behalf of themselves as persons subject to due diligence under the SPG.

The information, data, and necessary documents gathered from the policyholder must then be transmitted to the delegating insurance undertaking. In these cases, it is sufficient for the insurance broker to make copies of the relevant documents and data for the broker's own due diligence files and to indicate from the records when the documents and information were transmitted to the insurance undertaking.

Sub-delegation, however, is excluded according to Article 24(3) SPV. As a result, due diligence obligations that have already been delegated by the insurance company to the insurance broker (delegation) cannot be delegated again by the insurance broker to a third party (sub-delegation).

4. Internal organisation

Upon being granted a licence as an insurance broker for life insurance, insurance brokers must take appropriate internal organisational measures to ensure compliance with the provisions of the SPG and the associated SPV at all times. The internal organisation must be structured overall according to the type and size of the enterprise as well as according to the number, type, and complexity of the business relationships. This obligation applies regardless of whether life insurance has already been brokered or not.

Asset management companies (Article 3(1)(i) SPG)

1. General remarks

In the course of the transposition of the EU Anti-Money Laundering Directive, the previous Article 10(1)(i) SPG and the corresponding legal fiction were repealed, so that asset management companies must in principle apply the regular due diligence obligations as persons subject to due diligence.[32]

1.1 Risk-mitigating factors

In line with Article 9a SPG, the person subject to due diligence may take risk-mitigating factors into account. When engaging in portfolio management, asset management companies – unlike banks – do not hold the client's assets themselves, but rather only have access to the client's custody account through a power of attorney for investments. The asset management company buys and sells financial instruments for the client from existing assets for the client's account, but has no influence on inflows or outflows of assets. For certain services provided by an asset management company (e.g. investment advice without a client power of attorney or securities and financial analysis), the company has no access to the client's custody account. For this reason, the usual activities of an asset management company can generally be assumed to entail reduced risks. However, this does not lead to application of simplified due diligence, but rather to the consideration of reduced SPG risks in the context of the application of regular due diligence. Where the relevant aspects apply (see point 1.2 below), asset management companies must perform increased due diligence.

1.2 Enhanced due diligence (Article 11 SPG)

In cases where there is an increased risk of abuse of money laundering, organised crime, or terrorist financing, a stricter standard of due diligence obligations (i.e. enhanced due diligence) must be applied.

The classification of business relationships according to a risk-based approach must in principle be carried out individually by the persons subject to due diligence. Non-exhaustive criteria to be considered for business relationships and transactions with increased risks are listed in Article 11 SPG and Annex II to the SPG. As part of the risk assessment, an asset management company must check in particular whether the following criteria are met:

- Is the contracting party or beneficial owner a politically exposed person (PEP)?
- Is any legal entity serving as the contracting party a recognisably complex structure or does it exhibit a similar pattern?
- Is the residence/habitual abode of the contracting party or beneficial owner[33] in a country with strategic deficiencies or higher geographic risks in accordance with List A[34]?
- Is there an increased transaction volume?

When performing enhanced due diligence, asset management companies must in particular ensure more intensive ongoing monitoring as well as a business profile that satisfies the increased risks (Article 8 SPG and Article 20 SPV).

2. Business profile, ongoing monitoring of business relationship, and PEPs

Pursuant to Article 8 SPG and Article 20 SPV, the persons subject to due diligence must establish a business profile. The level of detail of the business profile depends on the degree of risk in the business relationship

[32] Pursuant to the Law of 4 May 2017 amending the Due Diligence Act, Article 10, Article 11(1), (2), and (7) SPG, the second sentence of Article 22(1), and Article 22(3) SPG enter into effect on 1 March 2018 and Articles 16, 20, and 20a SPG on 1 June 2018.
[33] In the case of foundations and trusts, as well as corporate bodies held by foundations or trusts, it is sufficient to take into account the residence of the effective founder, settlor, or trustor.
[34] https://www.fma-li.li/files/fma/fma-rl-2013-1-liste-a.pdf

(Article 20(2) SPV). When applying regular due diligence obligations, asset management companies may take risk-mitigating factors into account in their preparation of the business profile.

Moreover, pursuant to Article 5(1)(d) and Article 9 SPG, persons subject to due diligence must also monitor their business relationships, including the transactions carried out in the course of the business relationship, at a level that is commensurate with the risks involved.

When applying regular due diligence, asset management companies may structure the ongoing monitoring of business relationships in accordance with the risk-mitigating factors listed in point 1.1. Nevertheless, a business relationship in the normal course of business activity (e.g. portfolio management; the applicable requirements for asset management companies in the course of business activity are set out in the Asset Management Act and Asset Management Ordinance) must be given appropriate due diligence attention. If circumstances or transactions arise that deviate from the business profile, simple investigations must be carried out with reasonable effort in accordance with Article 9(3) SPG. If circumstances or transactions arise which give rise to suspicion that assets are connected with money laundering, predicate offences of money laundering, organised crime, or terrorist financing, special investigations must be carried out in accordance with Article 9(4) SPG.

If, in the course of the business relationship, a suspicion of money laundering, a predicate offence of money laundering, organised crime, or terrorist financing arises, the asset management company must immediately comply with its reporting obligation under Article 17 SPG. The responsibility for submitting the report lies with the member of the executive body designated to ensure compliance with the SPG.

This guidance takes precedence over the guidance governing the business profile and ongoing monitoring in the General Part of this Instruction and conclusively governs the interpretation of the corresponding provisions for asset management companies.

The provisions on PEPs set out in Article 11(4) SPG also apply in principle to asset management companies. Contrary to the guidance in point 6 of the General Part of this Instruction, the following applies to asset management companies:

- the PEP check for asset management companies does not cover recipients of distributions, given that asset management companies do not have to identify recipients of distributions, as described in point 4 below; and
- in the case of asset management companies, it is sufficient if the documentation of the PEP check is carried out by a third party (e.g. the principal bank), provided that this third party fulfils the requirements of Article 14(1)(a) or (b) SPG in conjunction with Article 24 SPV. In the case of delegation, however, responsibility for the PEP check remains with the asset management company.

The principles for risk-appropriate monitoring of business relationships are to be implemented as written procedures in the internal SPG instruction or in the organisation manual.

3. Asset management for a fund

By way of introduction, it is important to clarify that there are two levels of due diligence for undertakings for collective investment (UCIs). A distinction must be made between (1) a business relationship with the UCI and (2) a business relationship with the subscribing persons.

Only the UCI maintains a business relationship with the subscribing persons. The other persons subject to due diligence who provide services to the UCI (e.g. depositary, asset manager, etc.) only have a business relationship with the UCI itself. On the part of the other persons subject to due diligence, the UCI must therefore be identified and verified as a contracting partner according to Article 6(1) SPG.

As explained in FMA Communication 2018/07 on UCIs, a UCI has to identify either the subscribing institutions or the ultimate investors (in whose interest the subscription is ultimately made) as beneficial owners when dealing with the subscribing persons, depending on the risk assessment at the level of the business

relationship as well as at the level of the UCI. The provision in Article 22b(3) SPV is therefore directly relevant only for the UCI.

Insofar as the UCI is allowed to apply Article 22b(3) SPV for the determination of the BO, this is, however, also indirectly relevant for the other persons subject to due diligence.

In principle, the provisions under Article 3(1)(a) (e.g. SICAV) and (b) (e.g. collective trusteeship) of the Due Diligence Ordinance are authoritative for the other persons subject to due diligence when determining the beneficial owners of the UCI. If the UCI comprises several sub-funds, the relevant unit holders (≥25%) must be determined at the level of the sub-fund with which the depositary, asset manager, etc. has a business relationship.[35] In the case of a collective trusteeship with sub-funds, only the beneficiaries of the sub-fund with which the depositary, asset manager, etc. maintains a business relationship are relevant.

In order to determine the BO of the UCI, the depositary, the asset manager, etc. shall, on the one hand, question its contracting partner (the UCI) and, on the other hand, take into account any information available to the institution itself on the ultimate investors.

Applicability of Article 22b(3) SPV

If the UCI is allowed to apply Article 22b(3) SPV when applying the due diligence obligations to the unit subscribers, the UCI will be asked about the depositary, asset manager, etc. subject to due diligence with regard to unit holders (≥25%) according to Article 3(1)(a)(1) SPV and/or beneficiaries within the meaning of Article 3(1)(b)(4) SPV. The UCI must respond by stating in writing that Article 22b(3) SPV has been applied and that no ultimate investors have been identified.

As mentioned above, the depositary, the asset manager, etc. must not rely exclusively on the written information provided by the contracting partner (the UCI), but shall also take into account any such information available to the institution itself on the ultimate investors as may prevent the applicability of Article 22b(3) SPV at the level of the UCI (in particular, the criteria set out in II. Special Part for UCIs). This may be the case, in particular, if, for example, the asset manager or the depositary also acts as the promoter. In particular, the ML/TF risk that the depositary, asset manager, etc. has assigned to the business relationship on the basis of the risk assessment according to Article 9a SPG must also be taken into account here. If no relevant information is available, an active enquiry is only necessary if the UCI does not provide the asset manager with a confirmation of the application of Article 22b(3) SPV.

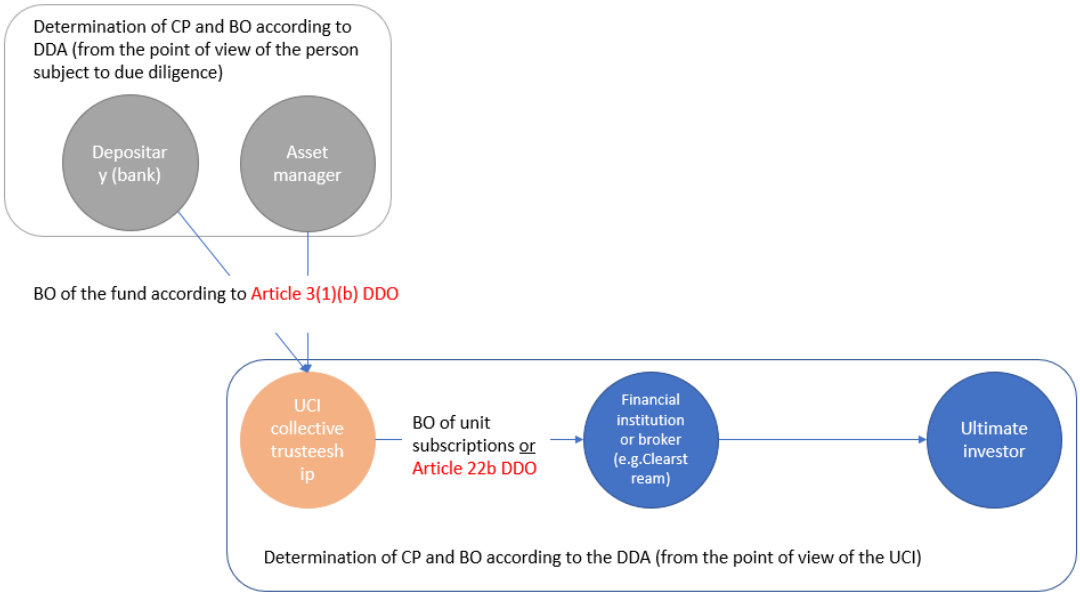
Even in the case of written confirmation by the UCI, the responsibility for determining the beneficial owner remains with the asset management company (depositary, etc.).
Under Article 7(3) SPG, persons subject to due diligence must repeat the identification and verification of the identity of the beneficial owner if doubts arise over the course of the business relationship concerning the identity of the beneficial owner. In the case of business relationships of asset management companies with funds according to Article 22b(3) SPV, the FMA considers it risk-adequate if this repetition takes place within the framework of the periodic risk assessment by way of a new confirmation of the UCI (the management company).

Irrespective of the applicability of Article 22b(3) SPV, at least regular due diligence must be applied by the asset management company when managing assets for a fund.

Non-applicability of Article 22b(3) SPV

[35] Cf. analogous due diligence approach with segmented association persons (protected cell companies).

If the UCI is not permitted to apply Article 22b(3) SPV, the other persons subject to due diligence shall identify the unit holders (≥25%) within the meaning of Article 3(1)(a)(1) SPV and/or the beneficiaries within the meaning of Article 3(1)(b)(4) SPV. If the UCI comprises several sub-funds, the relevant unit holders (≥25%) (as mentioned in the introduction) must be determined at the level of the sub-fund with which the depositary, asset manager, etc. has a business relationship. In the case of a collective trusteeship with sub-funds, only the beneficiaries of the sub-fund with which the depositary, asset manager, etc. maintains a business relationship are relevant.



The simplifications under Article 22b(3) SPV are, in particular, not applicable to investment companies pursuant to the Investment Undertakings Act (IUA), UCIs that are used for individual asset structuring, non-equivalent third-country funds without marketing authorisation in the EU/EEA or in the case of subscriptions by institutions from a non-equivalent third country and/or high-risk country (cf. Annex 4 SPV).

In connection with UCIs which may no longer apply Article 22b(3) SPV in the context of the reassessment of existing business relationships, reference is made to Chapter II Undertakings for Collective Investment, 2.1.3, regarding the determination and verification of the beneficial owners.

4. Legal entities established on a discretionary basis

Pursuant to Article 7a SPG, when dealing with legal entities established on a discretionary basis, persons subject to due diligence must obtain sufficient information concerning the persons in whose interest the legal entity has primarily been established or is primarily operated. Asset management companies are exempted from the additional obligation to identify the recipients of distributions pursuant to Article 7a SPG due to the risk-mitigating factors mentioned in the point above.

5. Financial analysis

In principle, asset management companies under Article 3(1)(i) are subject to due diligence with respect to all their business relationships. Within the scope purely of a financial analysis (without investment advice or other activities referred to in Article 3(1) VVG), the activity of the asset management company is limited to the analysis and, as part of this activity, it has neither power of attorney to manage the client's assets nor does it have knowledge of the origin of the assets. An asset management company therefore has no

obligation to identify the contracting party or the beneficial owner in a purely financial analysis as explained above or to carry out risk-appropriate monitoring. These due diligence obligations must be fulfilled only if, after the initial conclusion of the financial analysis agreement, an additional activity beyond purely financial analysis (i.e. an activity subject to due diligence as referred to in Article 3(1) VVG) is included in this business relationship.

FMA

Service providers for legal entities including liquidators (Article 3(1)(k) SPG, TCSPs)

1. Terminology

- **For the account of third parties** means that the person taking over an activity carries out this activity on behalf of or in the interest of and/or on the instructions of a third party.
- **Officially appointed liquidators** are generally appointed by the Commercial Register and are a member of the administration. They meet the requirements of Article 180a PGR or, as a legal person, have a licence under Article 14(1) of the Trustee Act (TrHG). If a legal person no longer has any governing bodies that meet the requirements under Article 180a PGR, the Commercial Register is responsible for appointing a liquidator. If there are good reasons, the Commercial Register may appoint another suitable person as liquidator upon application or *ex officio*.
- **Regularly appointed liquidators** are persons who do not have to be members of the administration of the legal person concerned, but who meet the requirements of Article 180a PGR. If they are legal persons, they must have a licence under Article 14(1) TrHG. These persons must, however, be appointed by a resolution of the supreme governing body of the legal person. This is often the person who has already held the function under Article 180a of the Persons and Companies Act (PGR).

2. Addressees (Article 3(1)(k) SPG)

2.1 General remarks

The guidance in this Special Part is addressed to natural and legal persons which provide one of the following services on a professional basis for the account of third parties:

- establishment of companies or other legal entities;
- performance of the management or executive function of a company, the function of partner in a partnership or a comparable function in another legal person or appointment of another person for the aforementioned functions;
- provision of a head office, a business, postal or administrative address and other related services for a legal entity;
- performance of the function of a member of a foundation council of a foundation, trustees of a trust or a similar legal entity or appointment of another person for the aforementioned functions;
- performance of the function of nominee shareholder for another person, where the company concerned is not listed on a regulated market and subject to the disclosure requirements in conformity with EEA law or similar international standards, or appointment of another person for the aforementioned functions.

Provision of the above mentioned services gives rise to the duty of due diligence under Article 3(1)(k) SPG; the persons subject to due diligence concerned are referred to as service providers for legal entities. The professional exercise of the activity according to Article 3(1)(k) SPG, thus, entails due diligence.

2.2 Delimitation from lawyers, law firms, and legal agents (Article 3(1)(m) SPG)

Lawyers and law firms with a licence under the Lawyers Act as well as legal agents within the meaning of Article 108 of the Lawyers Act who are subject to Article 3(1)(m) SPG are subject to the supervision of the Chamber of Lawyers.

Lawyers and law firms with a licence under the Lawyers Act and legal agents who provide activities according to Article 3(1)(k) SPG act as service providers for legal entities and are subject to supervision by the FMA. They shall report the exercise of activities to the FMA in accordance with Article 3(3)(b) SPG (see Section 6). In practice, this will usually involve the exercise of “co-governing body activities” by a lawyer, which, being performed by a service provider for legal entities, must be subsumed under Article 3(1)(k) SPG (see, in

addition, to the comments on liquidators in Section 5.1). In this context, however, it should also be noted that a lawyer must not under any circumstances assume trusteeships (not even as a "co-trustee") or management mandates according to Article 180a PGR, as this is a reserved activity of trustees and trust companies according to Article 2(b) TrHG as well as persons according to Article 3 of the Law on the Supervision of Persons according to Article 180a PGR.

In addition to the explanations in Section 4.3, it is noted that the provisions on the provision of joint services within the meaning of Article 15 SPG do not apply in the case of cooperation between persons subject to due diligence according to Article 3(1)(m) SPG and Article 3(1)(k) SPG due to the different competent authorities. However, if both act as service providers for legal entities according to Article 3(1)(k) SPG and are, thus, subject to the supervision of the FMA, the provision of joint services is possible according to Article 15 SPG.

3. Territorial scope of application

Based on the principle of territoriality (see General Part, point 4), Liechtenstein due diligence law is not limited to legal entities domiciled in Liechtenstein. Consequently, the registered office of a legal entity for which service as a governing body is being performed is not decisive for the determination of due diligence. Thus, for example, a professional trustee is also obliged to exercise due diligence for a BVI Ltd if the professional trustee performs activities as a director in or from Liechtenstein.

4. Scope and application of due diligence

4.1 General remarks

The person subject to due diligence must in principle fulfil all due diligence obligations. According to Article 5(1) SPG, these are:

- identification and verification of the identity of the contracting party (Article 6 SPG);
- identification and verification of the identity of the beneficial owner (Article 7 SPG);
- identification and verification of the identity of the recipient of the distribution of legal entities established on a discretionary basis and the beneficiary of life insurance policies and other insurances with investment-related objectives (Articles 7a and 7b SPG);
- establishment of a business profile (Article 8 SPG); and
- supervision of the business relationship at a level that is commensurate with the risk (Article 9 SPG).

If a person is already subject to due diligence as a result of a different activity, no further due diligence obligations arise from an additional activity in the same business relationship (e.g. service as a governing body in addition to service as a representative office in the same business relationship). In particular, this means that in these cases no second due diligence file has to be kept or created for the same business relationship, provided that the due diligence records are located in Liechtenstein. This also applies to cases where the due diligence obligations for different due diligence activities are performed within the company or group by different domestic legal or natural persons, provided that the same business relationship is involved and the group is audited on a consolidated basis.

This does not affect any reporting obligations under Article 17 SPG.

Example: A group consists of three domestic trust companies A, B, and C. An employee of Trust Company A acts as a member of the foundation council alongside Trust Company B, and Trust Company C provides the representative office. In such a case, only one of the persons subject to due diligence has to maintain the due diligence file.

This interpretation regarding the company- or group-internal exercise of due diligence corresponds in general to Article 15(1) SPG (provision of joint services; see point 4.3). In contrast to the provision of joint services, however, compliance with the following conditions is not mandatory:

- provision of services using the same joint billing and the same business name (Article 15(1) SPG);
- access to the due diligence files at any time (Article 15(3)(a) SPG);
- written agreement (Article 15(3)(b) SPG);
- appropriate monitoring of the proper performance of duties (Article 15(3)(b) SPG).

Due to these simplifications, however, application of Article 31(8) SPG is not provided for. This possibility of exemption from penalty is limited to the provision of joint services under Article 15 SPG. Accordingly, if due diligence is performed within a company or group, all involved persons subject to due diligence are punished in the event of a breach of due diligence law, especially given that all are equally responsible for the performance of due diligence.

Because the company- or group-internal exercise of due diligence is an interpretation of Article 15(1) SPG, the guidance on the assumption of a mandate by a previously involved person subject to due diligence and on recordkeeping in the event of an assumption of a mandate in point 4.3 applies *mutatis mutandis*.

Persons and companies performing their activities on the basis of an authorisation under the RAG cannot make use of this exemption, provided they perform activities jointly with a person or company that operates on the basis of a licence pursuant to special legislation issued by the FMA.

4.2 Identification and verification of the identity of the distribution recipient (Article 5(1)(b^{bis}) SPG)

Already at the time of the establishment of a discretionary legal entity, the persons subject to due diligence must obtain sufficient information concerning the persons in whose interest the legal entity has primarily been established or is primarily operated. The information must be sufficient so that the person subject to due diligence will be able to determine the identity of the distribution recipient at the time of paying out (Article 7a SPG).

The same principles apply to the identification and verification of the identity of the distribution recipient as for beneficial owners (see General Part, point 5.3). In principle, the distribution recipient must be determined for each distribution using Form D and the identity verified by appropriate measures (Article 7a(2) SPG). A document with probative value as referred to in Article 7 SPG (e.g. passport copy) must be obtained to verify identity. Please also refer to FMA Communication 2015/7 concerning identification of the beneficial owners under the Due Diligence Act.

Service providers for legal entities which provide services pursuant to Article 3(1)(k)(2) or (4) SPG to a legal entity established on a discretionary basis must transmit, directly and without being requested to do so, the information obtained (Form D) to other persons subject to due diligence under Article 3(1) SPG, provided that the legal entity in question maintains a business relationship with those persons and the information relates to assets which are booked there. It is sufficient if the original Form D is sent to the other persons subject to due diligence and a copy remains in the service provider's own due diligence file.

4.3 Provision of joint services under Article 15 SPG

In principle, several persons subject to due diligence have the possibility of providing joint services, provided that the conditions of Article 15(1) or (2) SPG are met. This means that the due diligence obligations are performed by the person subject to due diligence who holds the mandate, working alone.

While Article 15(1) SPG applies to all due diligence activities, Article 15(2) SPG is limited to service as a governing body for the account of third parties as referred to in Article 3(1)(k)(2) and (4) SPG (see also the guidance in point 5.2). With respect to the "comparable function" referred to in Article 15(2) SPG, please note

that the other activities covered by Article 3(1), such as providing a representative office, cannot be subsumed under that term.[36]

Persons subject to due diligence who do not personally perform due diligence must ensure that:

- they are given access to the due diligence files at any time on request; and
- a person subject to due diligence is appointed by written agreement to perform the duties, and proper performance of the duties is verified appropriately. The written agreement must contain at least:
    - the name or business name of the person subject to due diligence holding the mandate;
    - the name or business name of the person subject to due diligence who does not personally perform due diligence;
    - precise description of the business relationships or occasional transactions for which due diligence is performed by the person subject to due diligence holding the mandate; and
    - rules governing right of access to due diligence files and appropriate verification of compliance.

For business relationships which already existed on 1 September 2017 and in respect of which the provision of joint services applies, the written agreement of the person subject to due diligence who does not personally perform the obligations must be obtained by 1 September 2018. The appropriate verification must take place once the written agreement is available.

The person subject to due diligence who does not personally perform the obligations is not punished if that person has designated a person subject to due diligence by written agreement to perform the obligations and appropriately verifies the proper performance of the obligations (Article 31(8) SPG). This provision also entails in particular that the responsibility for compliance with the due diligence obligations remains with the individual persons subject to due diligence, i.e. also with those who do not personally perform the due diligence.

With regard to the appropriate verification, the FMA is of the view that at least a random check of compliance with the due diligence obligations of the persons subject to due diligence holding the mandate must be carried out (e.g. based on the random checks defined in FMA Guideline 2013/2). Such random checks should be logged for the purpose of traceability. In order to be able to carry out the verification at all, the persons subject to due diligence who do not personally perform the obligations must ensure that they are given access to the due diligence files at any time upon request. This right of access must persist even after the business relationship has ended, namely for the duration set out in Article 20(1) SPG. This entails that those persons subject to due diligence who do not personally perform the obligations are in principle not obliged to keep any client-related or transaction-related documents and records within the meaning of Article 20(1) SPG.

Example: Two professional trustees domiciled in Liechtenstein each provide a member of a foundation council. Under the conditions mentioned above, one of the professional trustees may be "exempted" from the due diligence obligations.

If the person subject to due diligence holding the mandate withdraws from the group of persons subject to due diligence (e.g. due to termination of the employment relationship or death), the remaining persons subject to due diligence who so far have not personally performed due diligence must immediately appoint a new person subject to due diligence holding the mandate from among themselves, or each person must perform due diligence individually.

If the intention is for a person subject to due diligence from the group of persons subject to due diligence to take over the business relationship entirely – irrespective of whether this person is the person subject to due diligence holding the mandate or not – e.g. as a result of a change to another trust company, then this person is not obliged, in light of the person's previous duty of due diligence, to completely perform due diligence again, provided that the person can at least take over a copy of the due diligence files. Given the previous duty of due diligence, this does not qualify as a takeover of a mandate in which a business relationship is

[36] See remarks in Report and Motion No. 124/2008, 70-71 on the distinction between the activities subject to due diligence of "performing the function of a governing body" and "providing representative offices".

taken over by a person subject to due diligence who was not previously involved. Irrespective of this, continued use of the existing due diligence files is permissible only if they comply with the provisions of due diligence law, have been verified, dated, and signed (again).

Due diligence law does not contain any provision on the right to the surrender of the due diligence files vis-à-vis the person subject to due diligence who has so far kept the files. The FMA is of the view, however, that in the event of the termination of the provision of joint services, the person subject to due diligence taking over the mandate must at least be granted access to the due diligence file for the purpose of making copies in accordance with Article 15(3)(a) SPG so that ongoing performance of the mandate in line with due diligence law can be ensured.[37]

With regard to the safekeeping obligation of the other previously involved persons subject to due diligence after termination of the business relationship as referred to in Article 20 SPG, an assessment specific to each case is required. In some cases, it may suffice to grant a right to access the files.

With respect to company- and group-internal performance of due diligence, please refer to point 4.1.

The provisions on the provision of joint services as within the meaning of Article 15 SPG do not apply in the case of cooperation between persons subject to due diligence according to Article 3(1)(m) SPG and Article 3(1)(k) SPG due to the different competent authorities. However, if both act as service providers for legal entities according to Article 3(1)(k) SPG and are, thus, subject to the supervision of the FMA, the provision of joint services is possible according to Article 15 SPG.

5. Special aspects of the profession

5.1 Liquidators (Article 3(1)(k)(2) and (4) SPG)

A liquidator must be classified as a governing body of the legal person to be dissolved and is thus subject to due diligence under Article 3(1)(k)(2) or (4) when performing the mandate. Liquidators officially appointed by the Commercial Register in accordance with Article 133 PGR have the same duties and responsibilities in liquidation proceedings as liquidators regularly appointed in accordance with Article 132 PGR.

With regard to the performance of due diligence, however, it makes little sense under the purpose of the SPG for the liquidator to perform all due diligence obligations again for which the previous body was already obliged. This means that the liquidator must obtain access to the due diligence records when taking over the mandate. Should the due diligence records give rise to doubts as to the identity of the contracting party or the beneficial owner, the liquidator must again identify and verify the contracting party or the beneficial owner. If, in the liquidator's opinion, there is no doubt as to the identity, a new identification and verification by the liquidator is not necessary.

Furthermore, the liquidator has an unlimited obligation to monitor the transactions carried out in the course of the liquidation in a risk-appropriate manner. In addition, there is in all cases an obligation to submit a suspicious activity report to the FIU under Article 17 SPG if there is a suspicion of money laundering, a predicate offence of money laundering, organised crime, or terrorist financing.

In the event that the liquidator does not find any due diligence records relating to the mandate or is denied access, the liquidator must contact the FMA to determine further steps.

Liquidators appointed by the Court of Justice in the context of initiation of bankruptcy are not subject to due diligence for purposes of the SPG. Although the appointed liquidator may represent the bankrupt company similarly to a governing body, the liquidator may not recognise or settle claims without the court's approval. The liquidator is moreover obliged to obtain the court's instructions for important business transactions.

[37] According to the judgment of the Supreme Court of 13 June 2014, LES 2014, 181, the due diligence files are assigned to the person subject to due diligence and not to the legal person managed by that person subject to due diligence. To that extent, the persons subject to due diligence involved at least have the right to inspect the due diligence file concerning them.

If a lawyer is appointed as the official liquidator of a legal person to be dissolved, there is a duty of due diligence pursuant to Article 3(1)(m) SPG, so that responsibility for supervision and execution of the SPG does not lie with the FMA, but rather with the Liechtenstein Chamber of Lawyers (Article 23(1)(b) SPG).

5.2 Service as governing body for the account of third parties (Article 3(1)(k)(2) and (4) SPG)

Service as a governing body is subject to due diligence, as are comparable functions (e.g. function of a partner, general manager of a legal entity) exercised on a professional in a fiduciary capacity or for the account of a third party (Article 3(1)(k)(2) and (4) SPG). All other service as a governing body which is not performed for the account of third parties does not constitute an activity subject to due diligence.

"For the account of a third party" generally also means that the person who assumes service as a governing body in fact appears as the governing body, but instead of acting freely, acts on the instructions of a third party working in the background. A further criterion is the interest in which the service as a governing body is performed: If, for example, the purpose of the activity is to manage an operating company as the general manager, i.e. in the exclusive interest of the legal entity, and not to manage assets in the interest of a third party, the service is not for the account of a third party (see Report and Motion No. 124/2008, 31).

A third party may appear in various forms. Third parties may, for example, be beneficiaries of the legal entity or shareholders. In the case of shareholders, the delimitation may be difficult; however, acting for the account of a third party occurs when the shareholders carry out actions or give instructions which are actually reserved to the ordinary general management of the company and which go beyond the rights of shareholders. In the management of a foundation, a trust, or an establishment or trust enterprise structured in a foundation-like manner serving as an instrument for private asset management, the governing body generally acts in the exclusive interest of the beneficiaries, so that it can generally be assumed that it is acting for the account of third parties; this is true irrespective of the domicile of the legal entity.

The latter applies in particular to the assumption of a qualified function as a governing body under Article 180a PGR. In this case, it is always assumed that the service is performed for the account of a third party. This ensures that in legal entities which are not operating companies but primarily serve as instruments for private asset management or were established for public-benefit purposes, at least one person fulfils the due diligence obligations.

This means, for example, that the following situation does not fall under Article 3(1)(k)(2) or (4) SPG: A professional trustee/a person performs the service of a governing body in construction company XY. The person was appointed as a governing body of XY on the basis of (technical) abilities and qualifications (e.g. training as a master builder or special knowledge in the field of construction). The crucial factor here is that the person was appointed to the function on the basis of knowledge of the market, the industry, or the activity carried out. No person in the background is *de facto* acting on the governing body, but rather decisions are taken freely.

This means primarily that the governing bodies of operating companies which carry out a commercial activity should not be subject to due diligence. However, this applies exclusively to cases in which no service is performed as a governing body for the account of third parties within the meaning of Article 3(1)(k)(2) or (4) SPG. It is important in this regard that the governing body actually manages the undertakings and is free to make business decisions and is not subject to the instructions of a third party. As a rule, such undertakings have substance in the form of their own premises (office, warehouse, etc.) and their own employees.

The possibility of providing joint services under Article 15 SPG should be recalled here (see the guidance in point 4.3).

The establishment of signing authority on a bank account also creates due diligence obligations under Article 3(1)(k)(2) or (4) SPG, where the *de facto* possibility of signing is sufficient. However, it must be taken into account that for persons subject to due diligence only with signing authority (but without the status of a governing body or other function), the monitoring obligation applies only to the extent that they prepare or carry out such transactions for their clients.

A protector's due diligence arises if the protector is authorised, in accordance with his or her specific powers, to perform activities within the meaning of Article 3(1)(k)(2) or (4) SPG for the legal entity. If, for example, transactions may be carried out only with the consent or at the proposal of the protector, i.e. if the protector is involved in the administration of the legal entity, this in any case gives rise to a duty of due diligence. The same applies to the case where the protector is equipped with pure information rights but also with powers of approval with regard to the execution of transactions. Since in such a case the transactions are dependent on the protector's approval or can be prevented by the protector's veto, the protector has full insight into the financial situation of the legal entity and is involved in the settlement process. The protector accordingly has a decisive influence on the decision-making of the legal entity's governing bodies. However, it should be noted that the monitoring obligation applies to the protector only to the extent that the protector is involved in a given transaction.

If, however, the protector is not involved in the transactions of the legal entity, but only has the right, for example, to recall the governing body of the legal entity and to appoint new members, this is not an activity relevant to due diligence, given that there is no connection whatsoever with the settlement of transactions or the management of the business relationship.

If an emergency governing body is appointed so that a legal entity does not have to be liquidated for lack of a governing body when the active governing bodies resign at the same time, this emergency governing body must fulfil the due diligence obligations analogous to a liquidator. See also the comments above on liquidators. Consequently, in view of the purpose of the SPG, the emergency governing body does not have to again fulfil all the due diligence obligations to which the previous governing bodies were obliged. The emergency governing body must obtain access to the due diligence records. Should the due diligence records give rise to doubts as to the identity of the contracting party or the beneficial owner, the emergency governing body must again identify and verify the contracting party or the beneficial owner. Otherwise, no new identification by the emergency governing body is required. In addition, there is an unlimited obligation to ensure risk-appropriate monitoring. In all cases, there is an obligation to submit suspicious activity reports under Article 17 SPG.

5.3 Representative office (Article 3(1)(k)(3) SPG)

Article 3(1)(k)(3) SPG subordinates natural and legal persons to the SPG which act as a representative office for purposes of Articles 239 et seq. PGR.

If the actions of the representative are limited to the mere receipt, forwarding, and storage of declarations, notifications, and documents, there is an obligation to identify and verify the identity of the contracting party and the beneficial owner. The contracting party is the legal entity for which the representative office is provided. No business profile has to be created, and the obligation to carry out risk-appropriate monitoring does not apply, given the lack of a *de facto* possibility of carrying out monitoring. If the persons subject to due diligence have further duties and powers than those described above, the full due diligence obligations pursuant to Article 5(1) SPG come into effect as appropriate to these further duties and powers. Further powers include, for example, the opening or inspection of correspondence received. In such a case, the person subject to due diligence is in a position to carry out the necessary monitoring based on the powers of inspection.

The duty of due diligence is established as soon as a business, postal, or administrative address or other related services are provided. It is not necessary that the legal entities also have their registered office at the address provided. The provision of an address of service is sufficient to give rise to the duty of due diligence. Performance of the activities mentioned above is relevant only for legal entities, not for natural persons.

The obligation to submit reports under Article 17 SPG exists in any case.

5.4 Function of nominee shareholder (Article 3(1)(k)(5) SPG)

Article 3(1)(k)(5) SPG subordinates natural and legal persons which perform the function of nominee shareholder for another person, where the company concerned is not listed on a regulated market and subject to the disclosure requirements in conformity with EEA law or similar international standards.

If the function of a nominee shareholder is limited purely to the position of a partner or member, there is a duty to identify and verify the identity of the contracting party and the beneficial owner. The contracting party is the trustor, not the legal entity whose shares are held in trust. If, in practice, it is *de facto* impossible to monitor transactions when exercising purely the function of a nominee shareholder, the obligation to do so does not apply. In such a case, it is also not necessary to prepare a business profile. In any case, all transactions which are connected with the activity as a nominee shareholder must be monitored, such as dividend distributions. If the person subject to due diligence has more extensive duties and powers than those described above, the full due diligence obligations pursuant to Article 5(1) SPG shall apply as appropriate to those more extensive duties and powers.

The obligation to submit reports under Article 17 SPG exists in any case.

6. Notification of commencement of business activities (Article 3(3) SPG)

Lawyers and law firms with a licence under the Lawyers Act as well as legal agents within the meaning of Article 108 of the Lawyers Act who provide services according to Article 3(1)(k) SPG must immediately notify the FMA in writing of the commencement of their activities (Article 3(3)(b) SPG). The notification must be transmitted to the FMA at the latest within five working days upon commencement of activity (postage). The FMA provides the Form: Notification of commencement of activity relevant to due diligence on its website to make the notification.

Casinos (Article 3(1)(l) SPG)

1. Terminology

- **Occasional transaction:** In casino gambling, occasional transactions are defined separately in Article 135(2) of the Casino Ordinance (SPBV) and include:
  - the sale and redemption of chips or gaming tokens;
  - machine payouts;
  - the issuing and cashing of cheques;
  - exchanges of denomination or foreign currency and other cash transactions.
- **Business relationship:** Based on the definition in the General Part, the term "business relationship" is defined separately in Article 136(2) SPBV. According to this definition, a business relationship exists in particular if the casino provides the player with:
  - a chip custody account or a guest account;
  - an electronic carrier medium for game credits which is used for more than one day of gaming and has a credit balance of more than 5 000 Swiss francs;
  - a customer card which is recognised by the casino as a form of identification.
- **Identification** covers establishment and verification of the identity of a person in accordance with the identification method chosen by the casino (Article 25(2) of the Gambling Act (GSG) and Article 135 SPBV in conjunction with Articles 6 et seq. SPV).
- **Identification upon admission** as defined in Article 135(3) SPBV means the identification and documentation of each guest upon entry into the casino. To verify identity, the casino copies the probative document upon first entry into the casino or records it electronically. The casino defines these processes in its internal guidelines.
- **Threshold identification** as defined in Article 135(1) SPBV means the identification and documentation of the guest if, when carrying out occasional transactions as referred to in Article 135(2) SPBV an amount of CHF 2 000 is reached or exceeded. To verify identity, the casino copies the probative document upon first registration or records it electronically. The casino defines these processes in its internal guidelines.
- **Casino** as defined in the GSG is any undertaking (operator) licensed in Liechtenstein which, on a commercial basis, offers the opportunity for gambling, especially at game tables, gambling machines, or similar gaming equipment (Article 3(1)(q) GSG).
- A **gambling game** as defined in the GSG is a game offering the prospect of winnings in return for placement of a bet (Article 3(1)(f) GSG).

2. Addressees (Article 3(1)(l) SPG)

The guidance in this Special Part is addressed to casinos licensed under the GSG which, on a commercial basis, offer opportunities for gambling, especially at game tables, gambling machines, or similar gaming equipment.

These casinos are subject to the SPG (Article 3(1)(l) SPG) and the provisions of the due diligence legislation are applicable, unless the Gambling Act (GSG) or Articles 134 et seq. of the Casino Ordinance (SPBV) provide for special regulations to the contrary.

3. Territorial scope of application

Based on the principle of territoriality (see General Part, point 4), the due diligence activities carried out by casinos are always subject to due diligence if they are carried out in or from Liechtenstein. In principle, all activities are subject to the Due Diligence Act which consist in participation in gaming operations.

Irrespective of the principle of territoriality under the SPG, casinos licensed under the GSG may offer gambling games abroad in accordance with Article 7 GSG, provided this does not interfere with legal peace in relation with foreign countries.

4. Scope and application of due diligence

4.1 General remarks

The person subject to due diligence shall in principle comply with all due diligence obligations. These are in accordance with Article 25(2) GSG in conjunction with Articles 134 et seq. SPBV (cf. also Article 5(1) SPG and Articles 6 et seq. SPV):

- identification and verification of the identity of the player (Articles 135 et seq. SPBV);
- identification and verification of the identity of the beneficial owner (Articles 139 et seq. SPBV);
- creation of a business profile where business relationships under Article 136 SPBV exist (Article 141 SPBV); and
- risk-appropriate monitoring of the business relationship (Articles 142 et seq. SPBV).

This does not affect any reporting obligations under Article 17 SPG.

The extent to which the due diligence obligations must be fulfilled is determined by the risk inherent in the individual business relationship or occasional transaction. With regard to risk assessment and the application of the risk-based approach, please refer to the extensive guidance in FMA Guideline 2013/1 on the risk-based approach under due diligence law.

4.2 Enhanced due diligence obligations (Article 145 SPBV, Article 11 SPG, Annex 2 to Article 9a and 11 SPG)

In cases where there is an increased risk of abuse of money laundering, organised crime, or terrorist financing, a stricter standard of due diligence obligations must be applied.

The classification of business relationships according to a risk-based approach must in principle be carried out individually by the persons subject to due diligence. Criteria that may be considered for business relationships and transactions with increased risks are listed in Article 145(2) SPBV and in Annex 2 Section A SPG. However, these are neither conclusive nor mandatory. This means that the casino itself must define criteria in its internal instructions (see Article 145(1) SPBV) designating business relationships and transactions involving increased risks and correspondingly effective control and monitoring measures for risk mitigation in line with Article 11(1) SPG. In the case of business relationships and occasional transactions in accordance with Article 145(3) in conjunction with Article 11(4) to (6) SPG (contribution of CHF 30 000 or more in a single operation; business relationships and occasional transactions with politically exposed persons (PEPs); complex and unusually large transactions and transaction patterns that have no apparent financial purpose or discernible lawful purpose; business relationships and occasional transactions with contracting parties or beneficial owners domiciled in states with strategic deficiencies), enhanced due diligence obligations must be exercised.

On a supplementary basis, see the detailed guidance in FMA Guideline 2013/1 on the risk-based approach under due diligence law.

The following guidance on the individual due diligence obligations applies specifically to casinos in addition to or in some cases in derogation from the guidance in the General Part. In addition, the guidance in FMA Guideline 2013/1 on the risk-based approach under due diligence law must always be observed.

4.3 Identification and verification of the identity of the player (Article 135 SPBV, Article 6 SPG, Articles 6 et seq. SPV)

The identity of the player (for purposes of due diligence law) must be established for occasional transactions and business relationships and verified by inspecting a document with probative value. The identity document pursuant to Article 25 GSG must be valid within the meaning of Article 7 SPV.

Identification upon admission involves identifying all visitors as soon as they enter the casino for the first time and verifying them against a document with probative value. In the case of threshold identification, the due diligence identification of the player is triggered when an occasional transaction is carried out in accordance with Article 135(2) SPBV, provided the latter reaches the threshold amount of CHF 2 000 (Article 135(1) SPBV). If a business relationship exists, the player must be identified and verified when the business relationship is established (see Article 136(1) SPBV).

Irrespective of whether the casino applies threshold identification or identification upon admission, one-time identification and verification of the identity of the player is generally sufficient. Following identification, the casino must ensure that the transactions relevant to the threshold can be attributed to the player in question (who has already been identified), so that maintenance of a complete due diligence file can be ensured.

The verification of identity by inspection of a document with probative value is generally carried out by means of personal contact. In the case of business relationships without personal contact, personal identification and verification of identity may be replaced by suitable safeguards (Article 137(2) SPBV in conjunction with Article 14 SPV). In this context, please refer to the instruction on safeguards pursuant to Article 14 SPV.

4.4 Identification and verification of the identity of the beneficial owner (Articles 139 et seq. SPBV, Article 2(1)(e) and Articles 7 et seq. SPG, Articles 11 et seq. SPV)

The beneficial owner is always a natural person at whose instigation or in whose interest a transaction is executed or a business relationship is ultimately established.

Casinos must identify and verify the beneficial owner at the latest at the time when the player first makes an occasional transaction in accordance with Article 135(1) and (2) SPBV (Article 139(1)(a) and 2(a) SPBV). In the event that a casino uses the method of threshold identification according to Article 135(3) SPBV for the identification of players, the casino may also bring forward the identification of the beneficial owner to the time of first entry into the casino.

Following identification and verification of the identity of the beneficial owner, the casino must ensure that the results of the identification and verification of the beneficial owner can be attributed to the player in question (who has already been identified), so that maintenance of a complete due diligence file can be ensured.

Beyond this, the operator must also identify and verify the beneficial owner behind the player in the following cases:

- upon establishing a business relationship;
- the casino makes bank transfers in favour of the player; and
- when withdrawals are made from guest accounts.

If the beneficial owner originates from a country in which it can be shown that the information required under due diligence law is not used in official documents, the casino must take appropriate measures to verify the missing information. The casino shall document this for the specific player.

4.5 Risk-appropriate monitoring (Articles 142-143 SPBV, Article 9 SPG, Article 22 SPV)

The casino must appropriately monitor occasional transactions and business relationships on the basis of the risk assessment carried out under Article 9a SPG (Article 143(1) SPBV) in accordance with their individual risk and document those transactions and relationships for each player.

According to Article 143(3) SPBV, business relationships require permanent monitoring of the player and his or her transaction activity to ensure that the transactions comply with the business profile. For this purpose, the operator shall keep player-related documentation. Within the framework of the business profile, business relationships must be classified by risk categories (Article 141(2) SPBV).

Likewise, occasional transactions must be monitored and documented (Article 146 SPBV) for each player pursuant to Article 143(2) SPBV. The casino must monitor gaming operations in such a way that processes designed to prevent identification by artificially splitting the amounts ("smurfing") are detected and lead to the identification and registration of the guest concerned.

The business profiles of business relationships must be classified by risk categories (Article 141(2) SPBV). The following criteria, in particular, provide indications of an increased risk in business relationships and occasional transactions (Article 145(2) SPBV; Annex 2 Section A SPG):

1. the registered office or place of residence of the player and the beneficial owner or their nationality;
2. the nature and location of the business activity of the player and the beneficial owner;
3. the value of the assets exchanged, bet, or deposited;
4. the value of the assets exchanged back;
5. payments of more than 100 000 Swiss francs from chip custody accounts, guest accounts, or electronic carrier media for game credits;
6. a significant deviation from the customary transaction types, volumes, or frequencies;
7. a significant deviation in the transaction from the business profile in terms of type, volume, or frequency;
8. the country of origin or country of destination of transfers for the benefit of the player;
9. complex and unusual transactions;
10. contribution of CHF 30 000 or more in a single operation.

The operator must intensify its monitoring of business relationships and occasional transactions involving increased risk. Special attention must also be paid to risks arising from the use of new technologies (Article 9(2) SPG).

According to Article 145(3) SPBV, increased risks must always be assumed in the cases mentioned in Article 11(4) to (d) SPG or in the case of a contribution in a single transaction of CHF 30,000.00 and more (cf. Section 4.2 Enhanced due diligence).

4.6 Check with regard to politically exposed persons (PEPs)

With reference to the explanations in the General Part of this Guideline, the casino must verify for politically exposed persons (PEPs) whether the player and/or the beneficial owner is a politically exposed person.

This PEP check must be done when a business relationship is established or when an occasional transaction of CHF 2,000.00 or more is executed (Article 143(2) SPBV). Since PEP checks must be repeated at least annually, casinos must run a new PEP check if a player reaches the threshold value of CHF 2,000.00 (Article

143(2) SPBV) again after one year (after the first PEP check). This regulation must be understood as a minimum requirement and, if necessary, automated annual PEP checks can be implemented in IT terms after the first PEP check.

PEP checks must also be done when a business relationship is terminated (cancellation of the chip custody account and/or a guest account).

4.7 Refusal to carry out an occasional transaction and discontinuation of a business relationship

If due diligence cannot be performed, the person subject to due diligence must not enter into the business relationship and/or carry out the desired transaction (Article 5(3) SPG).. Likewise, an existing business relationship must be terminated if the due diligence obligations cannot be fulfilled. In this case, the termination must be accompanied by sufficient documentation of the outflow of assets. See also the guidance in the General Part.

In these cases, the casino may have to obtain special clarification according to Article 9(4) SPG and check whether a suspicious activity report according to Article 17(1) SPG has to be submitted to the Stabsstelle FIU (Article 142 SPBV) or whether the transaction has to be abandoned according to Article 18 SPG. Possible indicators of money laundering, organised crime, and terrorist financing are listed in Annex 3 SPV, which may give rise to the need for special investigations. Such suspicious facts may include situations when:

- a player presents false identity documents;
- several identity documents from different countries are issued in the name of the player;
- a chip custody account is opened under a different name;
- a player requests customer cards from the casino under a different name.

Further indications or suspicious facts may also arise from the transactions carried out by a player, in particular if they indicate an unlawful purpose or the financial purpose is not discernible or the transactions appear to have no financial purpose. Examples of this include:

- purchase of a substantial amount of chips by players who leave the casino without playing;
- deceptive transactions using cashless cards;
- if it becomes known that players are making loans to other players.

In addition, indicators exist in the case of transactions that are incompatible with the casino's knowledge and experience of the player. Such a situation may arise in particular if a player, contrary to their previous playing behaviour, suddenly and without plausible reason massively increases their bets or chip purchases or if the amount of the bets deviates significantly from the financial possibilities indicated by the information provided to the casino.

In general, greater attention must be paid to cash flow management, especially the fight against smurfing. An example in the area of denomination switching is when larger amounts of small denomination banknotes or coins are exchanged into large denominations (or vice versa), or when multiple exchanges are made just below the identification threshold. Other areas include the exchange or redemption of money or chips by another player (a "mandated" guest) who is connected to the original player in a way that is not recognisable to the casino. Examples of this would be the successive increase of the slot credit during a slot machine game or the repeated purchase of tokens, followed by a minimal game and then redeeming the credit for banknotes when leaving the casino.

Qualified indicators or suspicious facts arise in all cases in which, for example, a player offers the responsible casino employee (e.g. shift manager at a table game) bribes in the form of chips for a change in the transaction recording form with the aim of reporting lower transactions. The same applies to the request of casino guests for the issue of a confirmation of non-achieved game winnings, the payment of game winnings in foreign currency, or the request to pay out game winnings to a third party.

Appropriate internal processes must ensure that indicators and suspicious facts are investigated immediately, leading to concrete measures by the casino.

5. Special aspects of the profession

5.1 Due diligence concept (Article 11 GSG in conjunction with Article 148 SPBV)

Operators are obliged to maintain a due diligence concept which ensures that the due diligence obligations are fulfilled. The due diligence concept must consist mainly of three components: obligation to identify, monitor, and organise.

5.2 Admission (Article 40 SPBV)

Before a player is admitted to gaming operations, the operator must check the player's identity against the lists of persons subject to a gaming ban (Article 22 GSG; Articles 40, 58, and 142 SPBV). In order to comply with the identification obligation under Article 25 GSG, the operator of a casino must therefore identify all persons and match them with the list of gaming bans and the ISG sanctions lists (lists of persons and countries against which sanctions have been imposed in accordance with the International Sanctions Act) before granting admission to the casino.

From the moment of admission to the casino, the player as a person and the player's transaction activity are subject to constant monitoring by the operator (due diligence obligations). Details are discussed under the preceding points.

5.3 Means of payment and financial transactions (Article 30 GSG)

5.3.1 Non-negotiable cheques (Article 150 SPBV)

With the exception of non-negotiable cheques, the casino may not accept or issue any other type of cheque. If it issues or accepts non-negotiable cheques, it must register the information in accordance with Article 44(1)(a) to (d) SPBV and keep a register of the non-negotiable cheques received and issued (Article 150(1) SPBV).

In the case of a cheque transaction with increased risk in accordance with Article 143(3)(c) in conjunction with Article 145 SPBV, the casino must take effective measures for additional, more intensive monitoring.

5.3.2 Chip custody account (Article 151 SPBV)

The casino may provide a chip custody account to a guest who does not wish to take or change their chips and gaming tokens before leaving the casino. This constitutes the establishment of a business relationship (Article 136(2)(a) SPBV) and obligates the casino, insofar as this has not already been done, to identify the player, to clarify his or her beneficial ownership of the assets and to draw up a business profile. In addition, the special documentation requirements under Article 44(2)(a) to (c) SPBV must be complied with.

If the business relationship involves an increased risk pursuant to Article 145(2) SPBV, the casino must apply the measures for intensified monitoring of the business relationship as laid down in the internal instructions. A case of increased risk must always be assumed *inter alia* in the case of a PEP in accordance with Article 145(3) SPBV in conjunction with Article 11(4) SPG.

The casino maintains a special register of chip custody accounts (Article 151 SPBV).

The chips issued by the casino entitle the player to play and/or exchange only in that casino. If the casino refuses to enter into a business relationship for the reasons set out in Article 5(3) SPG or if it terminates a business relationship that has already been entered into, the chip custody account must be dissolved and the assets repaid exclusively by issuing a non-negotiable cheque.

5.3.3 Guest account (Article 152 SPBV)

The establishment of a guest account gives rise to a business relationship in accordance with Article 136(2)(a) SPBV and is possible only in accordance with Article 152 SPBV. If such a business relationship is established without personal contact (Article 152(1) SPBV), the guest must submit the following documents to the casino using a form letter approved in advance by the Office of Economic Affairs:

- copy of the transfer order with the details of the executing bank and the account holder with the account number and address of residence;
- an authenticated copy of a probative document in accordance with Article 7 in conjunction with Article 9 SPV. If other measures enable the casino to verify the player, these measures must be documented, and the confirmation of authenticity may be waived;
- the declaration on beneficial ownership.

The casino must take appropriate measures to verify the player's address of residence and carry out a PEP check.

When withdrawals are made from guest accounts, the identity of the player and the beneficial owner must be established again and verified. The provisions of Article 152(3) and (4) SPBV in conjunction with Article 10(2) SPV apply *mutatis mutandis* to withdrawals and deposits.

If guest accounts are kept with the casino's principal bank in the form of a collective account, a complete list of the beneficial owners must be kept (Article 152(5) SPBV). If the casino refuses to enter into a business relationship for the reasons set out in Article 5(3) SPG or if it terminates a business relationship already entered into, the assets on the guest account must be transferred back to the bank that previously deposited the money.

5.3.4 Game winnings (Articles 42 and 43 SPBV)

Game winnings may be confirmed by the casino at the request of the player only in accordance with the provisions of Article 42 SPBV for table game winnings and Article 43 SPBV for gambling machine winnings. It must in all cases record the data in accordance with Article 44(3) SPBV.

5.3.5 Systematic documentation of payouts with voucher

Article 150(2) SPBV requires that non-negotiable cheques must be imprinted with “This document does not certify any bets or winnings” when issuing such cheques. The purpose of this provision is to reduce the risk of players requesting confirmations of winnings or other comparable confirmations/vouchers that can be used to make it appear to third parties that assets have been won in gaming operations and thus provide proof of origin. Against this background, similar to Article 150(2) SPBV, all confirmations/vouchers issued by the casino to a player (payout confirmation, winnings confirmation, payout tickets, transaction register, etc.) must be imprinted with “This document does not certify any bets or winnings” or “Not confirmation of any bets or winnings”.

In order to further counteract this risk and to carry out risk-appropriate monitoring in accordance with Article 142 SPBV, a complete record of the confirmations/vouchers issued to the players in accordance with the following list is required.

- Payout confirmation
- Confirmation of winnings
- Bank transfer
- Issuing of a non-negotiable cheque
- Handover of a copy of the payout ticket
- Issuing of a transaction register

- Other vouchers

Under this heading, complete documentation means that all payouts must be systematically recorded with a voucher – regardless of the amount.

The respective confirmations/vouchers issued in the course of a calendar year must be recorded in a register. In this register, the date of issue of the respective document, the name of the player, the date of birth, the nationality, the currency, the amount, the type of voucher and the employee of the casino who created the voucher for the player and/or carried out the transfer must be recorded.

6. Documentation and internal organisation

The following guidance on documentation and internal organisation applies specifically to casinos in addition to or in some cases in derogation from the guidance in the General Part.

6.1 Documentation (Article 146 SPBV; Article 20 SPG; Articles 27 to 29 SPV)

All forms, documents, and records that arise in connection with compliance with the provisions of due diligence law constitute the due diligence file of a player. The due diligence file includes in particular:

- documents and records which have served to identify and verify the identity of the player and the beneficial owner, in particular copies of the documents with probative value obtained for identification and verification;
- the business profile (in the case of a business relationship under Article 136 SPBV);
- the player-related documentation of occasional transactions and business relationships under Article 143(2) to (4) SPBV;
- any other records indicating transactions and, if applicable, the asset balance;
- documents and records on any simple and special investigations and any documents and records consulted in this connection (including in connection with cases of smurfing);
- the reasons for the application of simplified or enhanced due diligence obligations under Articles 10 and 11 SPG (alternatively, these reasons may be documented in other appropriate internal documents);
- records on the chip custody account in accordance with Article 151 SPBV and the guest account in accordance with Article 152 SPBV;
- documentation on the measures taken under Article 145(1a) SPBV; and
- copies of any reports submitted to the FIU under Article 17(1) SPG.

The customer-related documents, business correspondence, and supporting documents must be kept for ten years after the end of the business relationship or after the transaction has been completed. However, transaction-related records, business correspondence, and supporting documents must be kept for ten years after the transaction has been completed or after the record has been created.

6.2 Internal organisation (Articles 146 et seq. SPBV; 21 SPG; Articles 31 et seq. SPV)

6.2.1 Internal instructions (Article 149 SPBV; Article 21(1) SPG; Article 31 SPV)

The executive body of the casino must issue internal instructions for the concrete fulfilment of the due diligence obligations under due diligence law and bring them to the attention of all employees involved in business relations and occasional transactions.

The instructions must be formulated in such a way that they can serve as a guide for employees in the concrete exercise of due diligence obligations. This means it is usually not sufficient for the instructions to

merely reproduce the text of the law or ordinance. Rather, the persons subject to due diligence must formulate the internal instructions specifically for the requirements of gambling operations.

In particular, the internal instructions must set out:

- the processes, measures, and responsibilities referred to in Article 31(2)(a) to (d), (g), (i), and (k) SPV;
- the identification method chosen in accordance with Article 135 SPBV;
- the thresholds referred to in Article 143(2) SPBV;
- the criteria and measures referred to in Article 145(1a) SPBV; and
- the main features of basic and continuing training as referred to in Article 153 SPBV.

6.2.2 Basic and continuing training (Article 153 SPBV; Article 21(1) SPG; Article 32 SPV)

The casino must ensure that its employees receive up-to-date and comprehensive basic and continuing training, to the extent they perform activities subject to due diligence. In particular, all employees of the casino with money and guest contact and related tasks relevant to due diligence, as well as all persons responsible for the preparation and implementation of the due diligence concept (persons with management tasks relevant to due diligence law), are required to complete the mandatory basic and continuing training as referred to in Article 153(1) SPBV.

Depending on their functional level, casino employees who are subject to training must acquire the knowledge of the provisions of due diligence law, the manifestations of money laundering and terrorist financing, the internal measures to prevent money laundering and terrorist financing, as well as data protection that is necessary for the implementation of due diligence law.

Members of tax consultancy professions and external bookkeepers (Article 3(1)(n) SPG)

1. Terminology

- **Planning and execution of financial or real estate transactions** as defined in the SPG are, for example, cases in which assets are received or the transfer of assets is facilitated, for example by making accounts, custody accounts, or financial vehicles of any kind available.

2. Addressees (Article 3(1)(n) SPG)

2.1 General remarks

The guidance in this Special Part is addressed to natural and legal persons to the extent that they are professionally involved in the planning and execution of financial or real estate transactions for their clients in the context of their activities as members of tax consultancy professions or external bookkeepers, where such transactions concern:

- buying and selling of undertakings or real estate;
- management of client funds, securities or other assets of the client;
- opening or management of accounts, custody accounts or safe deposit boxes;
- procurement of contributions necessary for the creation, operation or management of legal entities;
- the management of trusts, companies, foundations or similar legal entities.

Provision of these services gives rise to the duty of due diligence under Article 3(1)(n) SPG as a member of a tax consultancy profession or external bookkeeper.

Members of tax consultancy professions may be (Article 2(1)(w) SPG):

- professional trustees and trust companies with a licence for the full exercise of activities;
- auditors and audit firms.

External bookkeepers may be (Article 2(1)(x) SPG):

- professional trustees and trust companies with a licence for the full exercise of activities;
- auditors and audit firms;
- persons with a licence under the Business Act as an accounting or controlling expert (bookkeeper).

Pure tax consultancy and bookkeeping without participation in the planning and execution of the financial and real estate transactions mentioned above is not subject to due diligence.

2.2 Delimitation from lawyers, law firms, and legal agents (Article 3(1)(m) SPG)

Where a lawyer performs tax consultancy activities, due diligence under Article 3(1)(m) SPG applies, so that competence for supervision and enforcement of the SPG is not allocated to the FMA, but rather to the Liechtenstein Chamber of Lawyers (Article 23(1)(b) SPG).

3. Territorial scope of application

Based on the principle of territoriality (see General Part, point 4), Liechtenstein due diligence law is not limited to legal entities domiciled in Liechtenstein. Consequently, the activities enumerated under point 3 are always subject to due diligence if they are performed in or from Liechtenstein, even if the legal entity, real property, or other asset is abroad.

4. Scope and application of due diligence

The person subject to due diligence must in principle fulfil all due diligence obligations. According to Article 5(1) SPG, these are:

- identification and verification of the identity of the contracting party (Article 6 SPG);
- identification and verification of the identity of the beneficial owner (Article 7 SPG);
- establishment of a business profile (Article 8 SPG); and
- supervision of the business relationship at a level that is commensurate with the risk (Article 9 SPG).

If a person is already subject to due diligence as a result of a different activity, no further due diligence obligations arise from an additional activity in the same business relationship (e.g. service as a governing body in addition to service as a representative office in the same business relationship). In particular, this means that in these cases no second due diligence file has to be kept or created for the same business relationship, provided that the due diligence records are located in Liechtenstein. This also applies to cases where the due diligence obligations for different due diligence activities are performed within the company or group by different domestic legal or natural persons, provided that the same business relationship is involved and the group is audited on a consolidated basis.

This does not affect any reporting obligations under Article 17 SPG.

Example: A group consists of two domestic trust companies A and B. An employee of Trust Company A acts as a member of the foundation council, and Trust Company B provides tax consultancy services to the foundation. In such a case only one of the persons subject to due diligence has to maintain the due diligence file.

This interpretation regarding the company- or group-internal exercise of due diligence corresponds in general to Article 15(1) SPG (provision of joint services; see Special Part on service providers for legal entities, point 4.3). In contrast to the provision of joint services, however, compliance with the following conditions is not mandatory:

- provision of services using the same joint billing and the same business name (Article 15(1) SPG);
- access to the due diligence files at any time (Article 15(3)(a) SPG);
- written agreement (Article 15(3)(b) SPG);
- appropriate monitoring of the proper performance of duties (Article 15(3)(b) SPG).

Due to these simplifications, however, application of Article 31(8) SPG is not provided for. This possibility of exemption from penalty is limited to the provision of joint services under Article 15 SPG. Accordingly, if due diligence is performed within a company or group, all involved persons subject to due diligence are punished in the event of a breach of due diligence law, given that all are equally responsible for the performance of due diligence.

Because the company- or group-internal exercise of due diligence is an interpretation of Article 15(1) SPG, the guidance on the assumption of a mandate by a previously involved person subject to due diligence and on recordkeeping in the event of an assumption of a mandate in point 4.3 applies *mutatis mutandis*. Persons and companies performing their activities on the basis of an authorisation under the Lawyers Act (RAG) cannot make use of this exemption, provided they perform activities jointly with a person or company that operates on the basis of a licence pursuant to special legislation issued by the FMA.

5. Special aspects of the profession

5.1 General remarks

According to Article 3(1)(n) SPG, external bookkeepers and members of the tax advisory professions are subject to due diligence if they are involved in the planning and execution of financial or real estate transactions for their clients that relate to the activities listed in Article 3(1)(m)(1) to (4) SPG or the administration of trusts, companies, foundations or similar legal entities. Bookkeepers or tax consultants become subject to due diligence only if they "actively" participate in such transactions by receiving assets or facilitating the transfer of assets, for example by making accounts, custody accounts, or financial vehicles of any kind available (Report and Motion No. 159/2016, 50). If this is not the case, the bookkeeper or tax consultant is not subject to the duty of due diligence under Article 3(1)(n) SPG.

For example, the mere activity of posting real estate transactions does not constitute "active" participation in real estate transactions. Likewise, pure tax consultancy is not subject to due diligence in connection with transfers of businesses if it does not "actively" participate in the transaction as described above.

5.2 Tax consultancy

Until the revision of due diligence law effective 1 September 2017, the declaration activity of completing a tax return was classified as subject to due diligence, but now no longer triggers due diligence obligations. This is because the mere completion of a tax return cannot, in principle, be connected with the "planning or execution of financial or real estate transactions", which fall under points 1 to 5 of Article 3(1)(m) SPG (Report and Motion No. 159/2016, 48).

The monitoring obligation is limited to those transactions where there is "active" participation of the tax consultant.

5.3 Bookkeeping

The term "external bookkeeper" (Article 3(1)(n) SPG) is further specified in Article 2(1)(x) SPG, referring to the fact that (bookkeeping) services are provided for third parties. This further specification is also reflected in the qualification "external', which refers to the fact that merely services for third parties are relevant, so that internal bookkeeping activity is exempt from due diligence (Report and Motion No. 159/2016, 38).

Accordingly, bookkeeping services provided by an employee of a company or by a group company for other group companies belonging to the group are exempt from due diligence, given that they are internal services.

The necessary data for the business profile can usually be derived from the purpose of the company for which the bookkeeping is performed,. Separate documentation of the business profile is not required, in light of the extract from the Commercial Register available for the purpose of identifying the contracting party. The monitoring obligation is limited to those transactions in which the bookkeeper "actively" participates.

Notwithstanding the remarks made under this point 5, reference should be made on a supplementary basis to Article 3(1)(k)(2) SPG, according to which service providers are obliged to perform due diligence for legal entities which on a professional basis perform the management or executive function of a company, the function of a partner in a partnership, or a comparable function in another legal entity. In the Special Part on service providers for legal entities, it is specifically stated in relation to Article 3(1)(k)(2) SPG that the establishment of signing authority on a bank account creates due diligence obligations in the same way as serving as a governing body for the account of a third party. The *de facto* power to trigger transactions suffices in this regard.

If, for example, a bookkeeper has been granted signing authority on the bank account of a company for which they are responsible for bookkeeping, the bookkeeper must comply with the due diligence obligations set out in Article 5(1) SPG. Accordingly, the identity of the contracting party and the beneficial owner must be established and verified, and a business profile must be created. Separate documentation of the business profile can generally be dispensed with, provided that an extract from the Commercial Register of the

company concerned has been presented. The monitoring obligation applies only to the extent that transactions are prepared or executed for customers.

6. Notification of commencement of business activities (Article 3(3) SPG)

Persons subject to due diligence under Article 3(1)(n) SPG, and accordingly members of tax consultancy professions and external bookkeepers that perform their activities pursuant to a licence under the Auditors and Audit Firms Act or the Business Act, must immediately notify the FMA in writing when they have commenced business activities (Article 3(3)(d) and (e) SPG). The notification must be transmitted to the FMA at the latest within five working days upon commencement of activity (postage). The FMA provides the Form: Notification of commencement of activity relevant to due diligence on its website to make the notification.

Persons subject to due diligence referred to in Article 3(1)(n) SPG are subject to the notification obligation set out in Article 3(3) SPG only to the extent that they are not already subject to due diligence supervision by the FMA in light of their licence under special legislation. The special legal authorisation must, however, include the activity of an external bookkeeper and/or tax consultant. However, as soon as this licence under special legislation no longer exists, a person subject to due diligence must comply with the notification obligation set out in Article 3(3) SPG if activities subject to due diligence continue to be performed, e.g. on the basis of a business licence as referred to in Article 3(3)(e) SPG.

Where persons subject to due diligence pursuant to Article 3(3) SPG which hold a licence under the Business Act discontinue their activities entirely, the FMA must be notified immediately in writing.

Real estate brokers (Article 3(1)(p) SPG)

1. Terminology

- **Real estate brokers** within the meaning of Article 3(1)(p) SPG are any individual or legal entity who, for remuneration, has the task of mediating the opportunity to conclude a contract in connection with the acquisition or sale and/or lease of real estate. This may include, for example, architects, civil engineers and building trustees.

2. Addressees (Article 3(1)(p) SPG)

The guidance in this Special Part is addressed to real estate brokers, to the extent that their activities include the acquisition or sale or lease of real estate insofar as the monthly rent amounts to CHF 10,000.00 or more. The provision of this activity gives rise to the duty of due diligence under Article 3(1)(p) SPG.

3. Territorial scope of application

Based on the principle of territoriality (see General Part, point 4), Liechtenstein due diligence law is not limited to legal entities domiciled in Liechtenstein. Consequently, the activities enumerated under Section 2 are always subject to due diligence if they are performed in and/or from Liechtenstein, regardless of whether the property or real estate is situated abroad.

Since implementation of the 3rd Anti-Money Laundering Directive (2005/60/EC) in March 2009, no distinction has been made any longer with regard to the acquisition or sale of domestic and foreign real estate. Therefore, any acquisition or sale of real estate is subject to due diligence.

4. Scope and application of due diligence

The person subject to due diligence must in principle fulfil all due diligence obligations. According to Article 5(1) SPG, these are:

- identification and verification of the identity of the contracting party (Article 6 SPG);
- identification and verification of the identity of the beneficial owner (Article 7 SPG);
- establishment of a business profile (Article 8 SPG); and
- supervision of the business relationship at a level that is commensurate with the risk (Article 9 SPG).

This does not affect any reporting obligations under Article 17 SPG.

5. Special aspects of the profession

In principle, those activities are to be covered by due diligence law in which the real estate broker at any time obtains the power to dispose of the assets of third parties, i.e. for example by receiving assets from the buyer/seller or by making the broker's account available for the settlement of a transaction. If this is not the case, the real estate broker has no duty of due diligence under Article 3(1)(p) SPG.

In the case of architects, engineers, or building trustees, the decisive factor for the activity to fall within the scope of due diligence is likewise the power of disposal over the assets of third parties in connection with the acquisition or sale of real estate. A pure brokerage activity, on the other hand, in which only the buyer and seller are brought together and which at most includes advice on the financing of a transaction, accordingly does not give rise to due diligence, provided that the broker does not at any time acquire the power of disposal over the assets of third parties.

When buying or selling real estate, both the buyer and the seller must be identified as contracting parties.

When buying or selling real estate, the beneficial owners must be identified on both the buyer and the seller side and verified on the basis of risk.

If there is no lasting business relationship as referred to in Article 2(1)(c) SPG, the preparation of a business profile in accordance with Article 8 SPG in conjunction with Article 20 SPV and risk-appropriate monitoring in accordance with Article 9 SPG may be waived. However, the contracting party and the beneficial owner must always be identified and verified on the basis of risk.

6. Notification of commencement of business activities (Article 3(3) SPG)

Persons subject to due diligence under Article 3(1)(p) SPG, and accordingly real estate brokers that perform their activities pursuant to a licence under the Business Act, must immediately notify the FMA in writing when they have commenced business activities (Article 3(3)(f) SPG). The notification must be transmitted to the FMA at the latest within five working days upon commencement of activity (postage). The FMA provides the Form: Notification of commencement of activity relevant to due diligence on its website to make the notification.

Where persons subject to due diligence pursuant to Article 3(3) SPG which hold a licence under the Business Act discontinue their activities entirely, the FMA must be notified immediately in writing.

Persons trading in goods (Article 3(1)(q) SPG)

1. Addressees (Article 3(1)(q) SPG)

The guidance in this Special Part is addressed to natural and legal persons who trade in goods on a professional basis, provided that payment is in cash or by means of a virtual currency or a token and the amount involved is CHF 10 000 or more. The provision of this activity gives rise to the duty of due diligence under Article 3(1)(q) SPG. The provision of services such as consultancy services does not fall within the scope of Article 3(1)(q) SPG.

2. Scope and application of due diligence

The person subject to due diligence must in principle fulfil all due diligence obligations. According to Article 5(1) SPG, these are:

- identification and verification of the identity of the contracting party (Article 6 SPG);
- identification and verification of the identity of the beneficial owner (Article 7 SPG);
- establishment of a business profile (Article 8 SPG); and
- supervision of the business relationship at a level that is commensurate with the risk (Article 9 SPG).

This does not affect any reporting obligations under Article 17 SPG.

3. Special aspects of the profession

In principle, all professional trading activities involving cash payments of CHF 10 000 or more are to be covered by due diligence law. A trader therefore becomes subject to due diligence irrespective of the sector, the person, and the activity carried out, provided that the criteria of activity on a professional basis and cash payments of CHF 10 000 or more are met.

It is irrelevant whether a transaction is carried out in a single operation or in several operations which appear to be linked. This means that where there is a material and temporal link between several separate transactions carried out by the trader with the same customer, these are regarded as a single transaction within the framework of a business relationship. If no lasting business relationship exists, transactions which are carried out in several operations and which appear to be linked must be considered as a single occasional transaction.

All transactions in which payment is made by other means (e.g. by bank transfer) are not subject to the provisions of Article 3(1)(q) SPG, nor, for example, is a private individual who sells a second-hand vehicle once and receives payment of more than CHF 10 000 (for lack of professional activity).

If there is no lasting business relationship as referred to in Article 2(1)(c) SPG, the preparation of a business profile in accordance with Article 8 SPG in conjunction with Article 20 SPV and risk-appropriate monitoring in accordance with Article 9 SPG may be waived. However, the contracting party and the beneficial owner must always be identified and verified on the basis of risk.

With regard to the special aspects of the profession in connection with virtual currencies or tokens, please refer to the guidance on TT service providers and other persons subject to due diligence with a nexus to services (Article 3(1)(r), (s), and (t) SPG) in the Special Part.

4. Notification of commencement of business activities (Article 3(3) SPG)

Persons subject to due diligence under Article 3(1)(q) SPG, and accordingly persons trading in goods that perform their activities pursuant to a licence under the Business Act, must immediately notify the FMA in writing when they have commenced business activities (Article 3(3)(g) SPG). Commencement of business activities is deemed to be the first action triggering due diligence obligations – i.e. the first acceptance of cash

payments in the amount of CHF 10 000 or more. The notification must be transmitted to the FMA at the latest within five working days upon commencement of activity (postage). The FMA provides the Form: Notification of commencement of activity relevant to due diligence on its website to make the notification.

Where persons subject to due diligence pursuant to Article 3(3) SPG which hold a licence under the Business Act discontinue their activities entirely, the FMA must be notified immediately in writing.

TT service providers (Article 3(1)(r) SPG) and other persons subject to due diligence with a nexus to TT services (Article 3(1)(s) and (t) SPG)

1. General remarks

The money laundering, organised crime, and terrorist financing risks associated with business relationships involving TT systems arise from the anonymity or pseudo-anonymity of transactions with virtual currencies or tokens, especially in regard to the beneficial owner of the assets, and from the fact that the bulk of these transactions are carried out internationally directly and without financial intermediaries and can therefore evade any form of control.
The risks manifest themselves both in the criminal exploitation of design flaws in virtual currencies and tokens and in investor fraud, especially in initial coin offerings (ICOs) and the use of virtual currencies or tokens for ransomware payments. However, the use of virtual currencies or tokens also poses a threat in other criminal patterns: terrorist financing, laundering of money from the sale of illegal services and products, phishing scams, or even drug trafficking, especially by criminal organisations. Their anonymity makes virtual currencies and tokens suitable for money laundering, organised crime, and terrorist financing.

However, these risks in business relationships involving systems are countered by additional possibilities for combating these risks compared with traditional financial transactions. These possibilities result directly from the use of TT systems and involve examining the history of the virtual currency or token in question ("technical origin of assets").

2. Terminology

- **Identification** means identifying and verifying the identity of a person using documents with probative value (Articles 6 et seq. SPV).
- **Virtual currency** means, according to Article 3(18) of the EU Anti-Money Laundering Directive and the identical formulation in Article 2(1)(z^{bis}) SPG, *"a digital representation of a value that was not issued or guaranteed by any central bank or public body and is not necessarily pegged to a legally established currency and does not have the legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange that can be transferred, saved and traded electronically."*
- **Token**, according to Article 2(1)(c) TVTG, means *"a piece of information on a TT System which:*
  1. *can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights; and*
  2. *is assigned to one or more TT Identifiers (an identifier that allows for the clear assignment of Tokens*[38]*)."*

It should be noted that the concept of "token" goes further than the concept of "virtual currency". For example, a "stable coin" whose value is linked to a legal tender (e.g. CHF) and which is issued against payment of an amount of money meets the definition of electronic money under Article 3(1)(b) of the Electronic Money Act. However, electronic money does not fall within the definition of "virtual currency" because it has the legal status of money. A "stable coin", on the other hand, regularly meets the requirements for a token (piece of information on a TT system; here, the token represents a value derived from the legal tender deposited; the token can be assigned to one or more TT identifiers).

[38] The relationship between a TT identifier and a TT key, which makes it possible to dispose of a token, is comparable to that between a safe deposit box and the corresponding key. Anyone who has the (TT) key can open the safe deposit box and take possession of its contents. The function of the TT identifier relates more to the safe deposit box or to the fact that a token can be assigned (see, generally, Statement of the Government to Parliament No. 93/2019, 23).

This also means that the classification[39] of a token is irrelevant to the subordination of TT services to the SPG.

3. Addressees (Article 3(1)(r), (s), and (t) SPG)

The guidance in this Special Part is addressed to TT service providers subject to due diligence and registration and to service providers subject to due diligence with a nexus to TT services. The performance of these activities gives rise to the duty of due diligence under Article 3(1)(g) to (t) and 3(3)(h) and (i) SPG. This covers the following service providers:

3.1 TT service providers subject to registration

3.1.1 Token issuer

According to Article 2(1)(k) TVTG, a token issuer is a natural or legal person who publicly offers tokens in their own name or in the name of a client.

- **Contracting party:** In the case of the token issuer, both the token buyer and the client are considered to be contracting parties for the issue, given that both must be regarded as placing the order in the sense of the terminology on the contracting party set out in point 2 of Section I.

3.1.2 TT key depositary

According to Article 2(1)(m) TVTG, a key depositary is a person who safeguards TT keys (e.g. private keys) for clients.

This means the TT key depositary has the *de facto* power of disposal over the token and also the authorisation to store the TT key. This gives the TT key depositary a limited power of disposal. Another form of limited power of disposal is the right to initiate transactions on behalf of the customer. It may also be possible for the TT identifier to be accessed via several TT keys. This means it is technically feasible to establish rules governing joint signature (see Report and Motion No. 54/2019, 67).

Typical example applications are (see Report and Motion No. 54/2019, 76-77):

- wallet providers, which store the TT key centrally on a server, thereby reducing the risk entailed by a possible loss of the smartphone;
- offline storage providers, which store TT keys separate from the internet in order to reduce the risk of hacker attacks;
- crypto-exchanges, which initiate the disposal of the tokens directly on behalf of the client via the TT key, allowing trading transactions to be carried out more efficiently.[40]

Ultimately, this means that any person who provides a service on a professional basis within the scope of which they have access to the TT key (private key) of a third party is considered a TT key depositary. This also applies, for example, to persons who, on a professional basis, manage assets[41] for third parties with regard to virtual currencies and tokens.

Persons are exempted who offer the safekeeping of physical wallets without having access to the key themselves (safe deposit services).

[39] e.g. as a payment token, utility token, or investment token, but note that Liechtenstein law does not establish criteria for the classification of tokens.
[40] These crypto-exchanges are thus deemed TT service providers subject to due diligence (Article 3(1)(r) SPG in conjunction with Article 2(1)(m) TVTG) and not operators of trading platforms for virtual currencies and tokens (Article 3(1)(t) SPG).
[41] This asset management does not fall within the scope of the Asset Management Act as long as no tokens are used that exhibit characteristics of a financial instrument under Annex 2 VVG.

3.1.3 TT token depositary

According to Article 2(1)(n) TVTG, a TT token depositary is a person who safeguards tokens in the name and on account of others.

The TT token depositary is of practical relevance in some applications. Firstly, this role is important for transaction accounts. Transaction accounts are used, for example, by crypto-exchanges, custodian banks, etc. to efficiently process a large number of transactions by many clients. The TT token depositary must assign all of its clients' tokens to one or several TT identifiers over which it has the power and right of disposal. The allocation to the customer is done in a – usually separate – database (see Report and Motion No. 54/2019, 77-78).

3.1.4 TT protector

According to Article 2(1)(o) TVTG, a TT protector is a person who holds tokens on TT systems in their own name on account for a third party. This is accordingly a service provider which provides typical fiduciary services within the framework of a TT system. A TT protector can therefore only be a professional trustee under the TrHG.

3.1.5 Physical validator

According to Article 2(1)(p) TVTG, a physical validator is a person who ensures the enforcement of rights in accordance with the agreement, in terms of property law, represented in tokens on TT systems. For example, a client may approach a token producer with the order to tokenise rights to an asset (e.g. a watch) which the client owns, by issuing a token over these rights to the asset. The physical validator ensures a link between the token and the right to property represented therein, for example by taking the watch into safekeeping and enabling the holder of the right of disposal over the token to exercise a right, such as the right of ownership by surrender (see Report and Motion No. 54/2019). The physical validator should clarify, in particular within the framework of the business profile, whether the assets in question correspond to the client's standard of living and subsequently clarify the origin of the assets. The process of tokenisation is generally not to be subsumed as an occasional transaction. It is rather a business relationship with all the associated due diligence obligations.

In a business relationship with a physical validator, the beneficial owner under Article 7 in conjunction with Article 2(1)(e) SPG is the natural person who is ultimately the beneficial owner of the right to be tokenised.

3.1.6 TT exchange service provider

According to Article 2(1)(l^{bis}) SPG, TT exchange service providers are natural or legal persons whose activities consist in the exchange of virtual currencies or tokens against legal tender or other virtual currencies or tokens and vice versa. According to Article 3(1)(r) in conjunction with Article 2(1)(q) TVTG, TT exchange service providers are subject to the SPG. It should be noted that the definitions of TT exchange service provider in the SPG and the TVTG are not entirely grammatically congruent. For the purposes of the SPG, the definition of the TT exchange service provider in Article 2(1)(l^{bis}) SPG applies as *lex specialis*.

The legal construct of the TT exchange service provider includes all service providers who change virtual currencies or payment tokens for other virtual currencies or payment tokens within their own books and hold neither tokens nor TT keys for customers (see also Report and Motion 54/2019, 102). TT exchange service providers do not cover service providers that exclusively conduct foreign exchange transactions. Such service providers are subject to the due diligence obligations as exchange bureau operators

TT exchange service providers which operate exclusively physical exchange machines have to comply with the due diligence obligations only when settling transactions of CHF 1 000 or more, regardless of whether the transaction is carried out in a single operation or in several operations which appear to be connected. The latter implies the following: A prerequisite for use of the relevant thresholds is that the persons subject to due diligence are able to detect if someone attempts to undermine the system by splitting a larger transaction (above the relevant threshold) into several smaller transactions (below the relevant threshold). This in turn requires that information is obtained for transactions even below the thresholds which makes it

possible to identify whether or not there is a connection with any further transactions below the thresholds. Such information can be systematically secured by using an automatic face recognition system, for example. Typical patterns for such procedures are e.g. short time intervals between transactions, the use of one and the same wallet, or transactions that are only just below the threshold value.

3.1.7 TT Agent

The TT agent is a person who professionally distributes or provides TT services on behalf of and for the account of a foreign TT service provider in Liechtenstein. The TT agent who has a registered office in Liechtenstein shall accordingly act on behalf of a TT service provider who does not have a registered office in Liechtenstein, by offering, distributing or providing the latter's products and services. The TT agent shall exercise due diligence in Liechtenstein as if he or she were providing the services himself or herself. However, the TT agent may also delegate the performance of due diligence to the TT service provider abroad in accordance with Article 24 SPV or outsource them in accordance with Article 24a SPV, provided that he or she has ensured that the performance of due diligence meets the Liechtenstein standard.

With regard to delegation and outsourcing, please refer to Chapter II, Insurance intermediaries, Section 3, of this Guideline.

3.2 Service providers with a nexus to TT services

3.2.1 Token issuers not subject to registration

This category includes token issuers not subject to the registration requirement set out in Article 12(1) or (2) TVTG (see point 3.1.1).[42]

Token issuers not subject to registration whose registered office or domicile is in Liechtenstein are subject to due diligence in accordance with Article 3(1)(s) SPG provided that they process transactions of CHF 1 000 francs or more, irrespective of whether the transaction takes place in a single operation or several operations between which there appears to be a connection.

Token issuers not subject to registration, but which are subject to due diligence as discussed above, must immediately notify the FMA in writing when they have commenced business activities. The FMA provides the Form: Notification of commencement of activity relevant to due diligence on its website to make the notification.

3.2.2 Operators of trading platforms for virtual currencies and tokens

According to Article 2(1)(z^{ter}) SPG, operators of trading platforms for virtual currencies and tokens are natural or legal persons who operate trading platforms via which their customers transact an exchange of virtual currencies or tokens against legal tender or other virtual currencies or tokens and vice versa, whose role is more than that of a simple intermediary without involvement in payment flows, but which do not store tokens or TT keys on behalf of their customers (Article 3(1)(t) SPG).

Purely decentralised trading platforms without an ability to intervene on the part of the operator must be viewed as equivalent to transactions between private individuals and are not subject to due diligence law (see also Report and Motion No. 54/2019, 103).

This means that "crypto-exchanges" may fall within the following categories of persons subject to due diligence:

- If the crypto-exchange manages the TT keys of its users, it is a TT key depositary (person subject to due diligence under Article 3(1)(r) SPG in conjunction with Article 2(1)(m) TVTG).

[42] Professional token issuers in Liechtenstein are subject to registration (Article 12(1) TVTG), as are token issuers with a registered office or place of residence in Liechtenstein who issue tokens in their own name or in the name of a client in a non-professional capacity, provided that tokens are issued in the amount of CHF 5 million or more within a period of 12 months (Article 12(2) TVTG).

- If the crypto-exchange manages the tokens of its users, it is a TT token depositary (person subject to due diligence under Article 3(1)(r) SPG in conjunction with Article 2(1)(n) TVTG).

- If the crypto-exchange manages neither the TT keys nor the tokens of its users and carries out exchange transactions with clients from its own portfolio, it is a TT exchange service provider (person subject to due diligence under Article 3(1)(r) SPG in conjunction with Article 2(1)(q) TVTG or Article 2(1)(l^{bis}) SPG).

- If the crypto-exchange manages neither the TT keys nor the tokens of its users and also does not carry out exchange transactions with clients from its own portfolio, but is able to influence the transactions of the users of the exchange, it is an operator of a trading platform for virtual currencies and tokens (person subject to due diligence under Article 3(1)(t) SPG in conjunction with Article 2(1)(z^{ter}) SPG).

Trading platforms for virtual currencies and tokens which are subject to due diligence as discussed above must immediately notify the FMA in writing when they have commenced business activities. The FMA provides the Form: Notification of commencement of activity relevant to due diligence on its website to make the notification.

4. Risk assessment

The persons subject to due diligence shall conduct a risk assessment to determine and assess the risks confronting them in respect of money laundering, organised crime and terrorist financing (Article 9a(1) SPG). The risk assessment must pay special attention to the factors for potentially lower or higher risk mentioned in Annexes 1 and 2 (Article 9a(2) SPG).

Taking into account the risk discussion in point 1 above, the following points suggest increased risks for TT services in any case:

Annex 2 Section A(b) SPG: Product, service, transaction or distribution channel risk factors:

- products or transactions that might favour anonymity (point 2)
- non-face-to-face business relationships or transactions, without certain safeguards as referred to in Article 14 SPV (point 3)
- new products and new business models, including new distribution mechanisms, and the use of new or developing technologies for both new and pre-existing products (point 5)

These risk factors, which are inherent in TT services *per se*, mean that there are no minor risks and that the application of simplified due diligence obligations under Article 10 SPG is therefore ruled out in this area.

TT services therefore exhibit at least normal risks and are accordingly at least subject to the application of regular due diligence obligations. However, the application of regular due diligence obligations requires that the risks inherent in TT services *per se* can be offset by factors and possible indicators of a potentially lower risk according to Annex 1 Section A SPG, e.g.:

- beneficial owners domiciled in lower risk geographical areas (Section A(a)(3))
- minor value assets and limited scope of transactions executed (Section A(a)(4))
- geographical risk factors (Section A(c))

If this is not the case or if there are even further factors and possible indications of a potentially higher risk (e.g. further factors according to Articles 11 and 11a SPG or (A) Annex 2 SPG), then increased risks are present and enhanced due diligence must be applied.

Where risk factors in Annex 1 or 2 SPG are based on "payments" (e.g. Annex 2 Section A(b)(4): payments received from unknown or unassociated third parties), these are to be considered as transactions in the

context of TT services. These factors must therefore also be taken into account for transactions of persons subject to due diligence who are TT service providers or service providers with a nexus to TT services.

Two types of transactions with virtual currencies or tokens with increased (pseudo-)anonymity can occur. In the first type, "normal" virtual currencies or tokens are used, but they are structured in a way that prevents information about the native distributed ledger of the virtual currency or token from being inspected. The second type uses virtual currencies or tokens that are specially designed to prevent the traceability of transactions on the public distributed ledger ("privacy coins").[43]

The money laundering, organised crime, and terrorist financing risk is even higher for the virtual currencies or tokens involved in TT services with increased anonymity compared with "normal" virtual currencies or tokens. The question arises in particular as to why there is a need for increased anonymity. Ultimately, each person subject to due diligence must decide for itself within the scope of TT services whether it wants to provide services involving virtual currencies or tokens with increased anonymity or not. In any event, the FMA urges great caution in this regard. As a rule, in addition to comprehensive business profiles, successful special investigations pursuant to Article 9(4) SPG will be necessary in order to be able to check the plausibility of the use of virtual currencies or tokens with increased anonymity. If no plausible use of virtual currencies or tokens can be shown, this will generally trigger an obligation to submit a report to the FIU under Article 17 SPG.

5. Business profile

The business profile pursuant to Article 8 SPG in conjunction with Article 20(1) SPV must also contain the TT identifier for TT services. The TT identifier is the technology-neutral term for the "address" or "public key". The requirements under Article 20(1) SPV are more directed at traditional financial business, such as fiduciary business or private banking, which tend to involve personal contact, a business relationship of long duration, and larger assets. TT services, in contrast, often take place without personal contact, are transaction-related, and tend to involve smaller assets.

For this reason, it is precisely the presentation of the (economic) origin of the assets that is a decisive factor in verifying the identity of the beneficial owner ("to satisfy themselves that the person in question is actually the beneficial owner") under Article 7(2) SPG.

The guidance on the business profile in the General Part of the Instruction applies in this regard. The following guidance in particular applies to the business profile:

- **Economic background of the total assets, including the profession and business activity of the effective contributor of the assets:** In the case of TT services, the profession of the beneficial owner must be stated in all cases. Without knowledge of the profession, the information on the economic origin of the assets can hardly be checked for plausibility. It should also be noted in this context that generic information such as "self-employed" or "employee" is not sufficient.
- **Intended purpose of the assets**: In the case of TT services, this can generally be found in the nature of the service. In the case of higher risks, additional and more detailed information must be captured in the business profile on the basis of risk.
- **TT identifier**: The business profile must include the TT identifiers belonging to the client, i.e. the public keys. If there are several TT identifiers, each must be contained/assigned in the business profile.

Documentation of the economic origin of the assets is especially important from the point of view of money laundering prevention. The question here is exactly how the assets involved in the TT service were generated. A risk-oriented approach can be taken in this respect. In the case of very small amounts, a blanket statement

[43] See also the remarks in Fincen Guidance FIN-2019-G001, 18.

such as "savings", "inheritance", "income from investment in fiat money", or "income from investment in virtual currencies or tokens" is sufficient. For larger amounts, the information must be more detailed and, where necessary, backed up by relevant documents. It is at the discretion of the person subject to due diligence to determine the thresholds above which information regarding the origin of the assets is to be obtained. These thresholds must in all cases be adapted to the risk of the specific business relationship.

The following table provides an example of risk-oriented documentation of the economic origin of assets. These thresholds can be considered to be risk-appropriate only if there are no other risk-increasing factors, however (e.g. CP/BO from List A countries, CP/BO from sensitive sectors, PEPs, complex structures, etc.). If risk-increasing factors are present, higher minimum requirements apply with regard to determining the origin of the assets/background of the total assets, given that the amount of the contributed assets represents only one of the numerous risk factors to be considered as a whole (in all such cases, at least the measures of the next higher level according to the table below must be applied; under certain circumstances, if several risk-increasing factors are present, it may also be necessary to apply measures above the next higher level).[44]

Amount	**Minimum requirement for "origin of assets" and "economic background of total assets"**
Level 1: Up to CHF 5 000 individual transactions (IT) Up to CHF 10 000 aggregate per year (APY)	• Brief descriptor of the origin of the assets and the economic background of the total assets such as "savings", "inheritance", "income from investment in fiat money", or "income from investment in virtual currencies or tokens" • Professional activity of the beneficial owner
Level 2: CHF 5 001 - CHF 25 000 IT CHF 10 001 - CHF 25 000 APY	Additionally: More detailed description of the economic origin of the assets (free text)
Level 3: CHF 25 001 - CHF 100 000 IT CHF 25 001 - CHF 100 000 APY	• Additionally: Clear description of the source and the amount (in ranges) of income and total assets of the beneficial owner • Additional relevant documents/records where necessary (see Section 5.4.2 of this Instruction)
Level 4: More than CHF 100 000 IT More than CHF 100 000 APY	Detailed business profile incl. relevant documents and records (see Section 5.4.2 of this Instruction)

6. Risk-appropriate monitoring

The persons subject to due diligence must monitor their business relationships, including the transactions performed in the course of the relevant business relationship, in a timely manner, at a level that is commensurate with the risks involved, to ensure that they are consistent with the business profile (Article 9(1) SPG). Depending on the TT service, risk-appropriate monitoring takes different forms:

[44] The enhanced due diligence described in Articles 11 and 11a SPG (especially in connection with politically exposed persons, complex structures/transactions and countries with strategic risks) must be applied independently of the obligation to clarify the origin of the assets on the basis of the threshold values listed in the table below.

6.1 Transaction monitoring for TT systems:

With regard to TT services, Article 21(2) SPV provides that in the case of business relationships or transactions with increased risks within the scope of enhanced due diligence, a suitable IT system for transaction monitoring must be set up, with which the transactions can be made traceable in the TT system used ("chain analysis").

Using the system, all transactions must be subjected to a sanction screening of the respective wallet address before completion of the transfer, which is defined by the power of disposition of the recipient, provided that the analysis supports the relevant TT systems.

The use of a system for checking the history of the virtual currencies or tokens (chain analysis) serves in particular to verify the information provided by a client with regard to the history of the virtual currencies or tokens and to determine whether these are virtual currencies or tokens with increased anonymity (see point 4 above), e.g. involving a "mixer" or "tumbler" for concealment.

The use of a system for verifying the history of the virtual currencies or tokens does not *per se* entail the plausibility of the economic origin of the assets, however, even though it may provide important elements in that respect.

6.2 PEP monitoring:

Effective 1 January 2020, TT service providers and service providers with a nexus to TT services subject to due diligence (Article 3(1)(r), (s), and (t) SPG) must in any case use an IT-based system to determine business relationships and transactions with PEPs, irrespective of the number of business relationships (last sentence of Article 21(1) SPV).

6.3 Exchange transactions by TT exchange service providers:

Transactions must be plausible in the context of the business profile. If there are any discrepancies, investigations must be undertaken. Systematic plausibility checks based on a chain analysis may also play a role here. Any necessary investigations must always be carried out before the transaction is executed – even if only a normal risk is assumed.

6.4 Crypto-exchange:

Here, exchange transactions are concluded under civil law via a smart contract between individual users of the trading platform. The person subject to due diligence must ensure, as part of risk-appropriate monitoring, that the transactions correspond to the business profiles. The person subject to due diligence must be able to identify deviations from the information provided at the establishment of the business relationship in terms of transaction volume or amount of assets involved.

6.5 Wallet providers (e.g. TT key depositaries):

As part of risk-appropriate monitoring of the wallet, the person subject to due diligence must ensure that the transactions correspond to the client's business profile. The person subject to due diligence must be able to identify deviations from the information provided at the establishment of the business relationship in terms of transaction volume or amount of assets involved.

6.6 Correspondent banking relationships:

Correspondent banking services do not only refer to correspondent banking services in the traditional financial market, but also those services that fulfil the aspects of correspondent banking services – so-called

correspondent bank-like services[45]. Such services are definitely also represented in the TT service market. This includes, for example, the execution of third-party payments in tokens or virtual currencies.

A TT service provider is a correspondent bank and/or correspondent bank-like, if it performs TT services for other TT service providers (respondent institutions). It does not matter whether the other TT service provider is domiciled in Liechtenstein or abroad. Such typical TT services may include the provision of liquidity, the provision of pass-through accounts, the making of payments or exchanges for clients of the respondent institution from tokens or virtual currencies to each other and/or to fiat money and vice versa, or similar services. Any TT service provider who carries out correspondent services for a third party does so within the framework of the client business relationship, unless the latter exceptionally carries out only a single transaction.

The respondent institution is the institution or the TT service provider that uses the services of the correspondent bank and/or the correspondent bank-like TT service provider.

Correspondent banking relationships pose a high risk, as it is sometimes not known for whom transactions are carried out. In this regard, correspondent banking relationships must be subjected to close continuous monitoring. Correspondent banking relationships must generally be approved by executive management. A due diligence check must be carried out as part of the onboarding process. This check includes at least an adverse media screening, a check of the effects with regard to predicate offences (e.g. by means of chain analysis tools), a check of the institution's beneficial owners as well as a check of whether the know-your-customer (KYC) and other due diligence obligations are complied with by the respondent institution and whether these are adequate with respect to Liechtenstein due diligence law[46]. Appropriate due diligence questionnaires[47] must also be obtained on a regular basis – at least every two years.
If the respondent institution is based in an at-risk country according to the Global Terrorism Index or in a country with strategic deficits, the business relationship should generally not be entered into and/or terminated. Otherwise, special attention must be paid to these transactions, with appropriate risk-mitigating measures, such as the transmission of KYC data to the client of the respondent institution.

6.7 Transactions to unhosted/private wallets:

Business relationships with transactions to an unhosted/non-custodial or private wallet[48] are characterised by the fact that such wallets are not subject to a KYC procedure. There is an increased risk in this regard, which also affects the business relationship. Risk-mitigating measures can be the assignment of the wallet to a known person by means of clustering or proof of ownership.

6.8 Internal transactions on a platform:

Sometimes on crypto exchanges not only trading against the crypto exchange is possible, but also peer-to-peer (P2P) trading. Business relationships that involve such internal transactions on a crypto exchange are subject to an increased risk, as such transactions are more difficult to trace and therefore also subject to increased continuous monitoring.

[45] See paragraphs 164 et seq. of the Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs of the FATF https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html. Correspondent bank-like services may also include the provision of payment services or the execution of fiat payments for TT service providers.
[46] Respondent institutions domiciled in the EU/EEA or countries under Annex 1 of this Guideline generally fulfil the equivalence requirement, unless they are listed in Annex 4 SPV.
[47] These questionnaires should be based on the Wolfsberg Principles: www.wolfsberg-principles.com/wolfsbergcb.
[48] Unhosted, non-custodial or private wallets are wallets for which no service provider is involved in the depositary service.

7. Documentation

The due diligence files contain in particular the documents and records prepared and consulted to comply with the SPG and the SPV. In the case of business relationships or transactions of persons subject to due diligence involving virtual currencies or tokens, the TT identifier referred to in Article 2(1)(d) TVTG must also be part of the due diligence files pursuant to Article 27(1)(d^{bis}) SPV. The TT identifier is the technology-neutral term for the "address" or "public key".

Depending on the TT service, it must be determined which TT identifiers are relevant. In the case of a TT exchange service provider, for instance, this is the TT identifier of the client who uses an exchange service. In the case of the operator of a trading platform, these are e.g. the TT identifiers of both parties which settle an exchange transaction via the trading platform. In addition, Article 27(1)(c) SPV stipulates that in connection with any investigations pursuant to Article 9 SPG, all documents and records consulted in this connection must be provided.

When TT services are provided, it is also necessary that the data storage for the entire TT system (blockchain data storage) be stored in the system of the person subject to due diligence to ensure that transactions can be traced where necessary. The person subject to due diligence[49] shall run a “full node” of the blockchain used. Only then is it possible to trace transactions independently and accurately. In addition, running a “full node” also allows for subsequent traceability, e.g. after a fork, etc. The data can be stored at a central location in the system of the person subject to due diligence and does not necessarily have to be kept in the due diligence file.

8. Internal organisation

The compliance officer, the investigating officer and the responsible member of the executive body as referred to in Article 22(1) SPG must have an in-depth knowledge in matters of the prevention and combating of money laundering, predicate offences of money laundering, organised crime, and terrorist financing as well as data protection law in connection with the token economy, and be familiar with the current developments in those fields (Article 36(1) SPV).

9. Simplifications in connection with token issues

9.1 Type of issue

When it comes to token issues, there are self-issues and third-party issues. In addition, there are differences as to whether the issue is subject to registration or merely subject to reporting. Third-party issues that are not subject to due diligence and registration are not relevant (for delimitation, refer to FMA Guidelines 2018/07 Chapter IX. Section 3).

9.2 Self-issues

A self-issue is usually a capital financing to implement the business idea. In any case, the issuer conducts the issue itself and has to apply due diligence – regardless of the amount invested – to all persons acquiring tokens.
However, taking into account the risk-based approach applicable in due diligence law, the issuer does not have to fulfil all organisational obligations under the SPG.
But, due to the inherent risks (cf. VNRA), the performance of certain duties is indispensable.
In terms of the organisation, it is essential that at least one person is responsible for due diligence. This person must be identified to the FMA using the reporting form for internal functions provided for this purpose.

[49] This refers, in particular, to service providers who offer depositary services or services via trading platforms.

This person must be a member of management of the company and combines all internal functions according to the SPG.
Usually, the issue involves an occasional transaction, and the issuer does not have an ongoing business relationship with an investor. Accordingly, the internal directives can be limited to the relevant points. Specifically, the internal directives must specify that investors must be accepted and how they must be accepted (onboarding process). For this, these specifications must be presented in a comprehensible manner and be accessible.
It is relevant to due diligence that information is obtained to the extent that the investor is, at least, identifiable (CP and BO determination and verification) and that the origin of the funds to be invested can be determined. In order to take account of the risk-based approach, it is also necessary to obtain third-party evidence to verify the plausibility of the origin of the assets in the case of large investors. Where investments can be made using cryptocurrencies, the risk of relevant transactions must also be clarified. The use of appropriate IT-supported systems (chain analysis) is recommended for such clarification.
The verification of plausibility and the existence of suspicious facts and any further clarifications as well as suspicious activity reports must be carried out by the person responsible for compliance with the SPG.

9.3 Third-party issues

It is equally true for third-party issues that the entire issuing activity is subject to due diligence.
As a rule, third-party issues are made in the course of the professional exercise of the activity. In this regard, all requirements under the SPG/SPV must be implemented accordingly. As it is usual to perform several issues, a relevant organisation, directives and training are also necessary and economically appropriate.

The connection to the principal of the issue usually qualifies as a business relationship in the case of third-party issues. In terms of investor connections, there will generally be an occasional transaction.

9.4 Overview of simplifications

The simplifications in connection with an issue can be summarised as follows:

Obligations	*Third party issue that needs to be registered (Art. 12 Abs. 1 TVTG)*	*Own issue that needs to be registered (Art. 12. Abs. 2 TVTG)*	*Third-party issue that needs to be reported (Art. 3 Abs. 3 SPG)*	*Own issue that needs to be reported (Art. 3 Abs. 3 SPG)*
Business profile	necessary	not necessary, if there is no business relationship	necessary	not necessary, if there is no business relationship
Risk Assessment, Transaction	necessary	necessary	necessary	necessary
Automatic PEP-Check/ Sanction Screening	necessary	at least manual PEP check	necessary	at least manual PEP check
Identification and verification of the CP	necessary	necessary	necessary	necessary
Identification and verification of the BO	necessary	necessary	necessary	necessary
Chain analysis	necessary when crypto assets are accepted	necessary when crypto assets are accepted	recommended	recommended
Clarifications	necessary	necessary	necessary	necessary
Suspicious activity reporting	necessary	necessary	necessary	necessary
Adverse media monitoring	media checks regarding high-risk investors	manual media checks regarding high-risk investors	media checks regarding high-risk investors	manual media checks regarding high-risk investors

Comprehensive internal functions	necessary	at least one person	necessary	at least one person
Internal Instructions	necessary	one-pager sufficient	necessary	one-pager sufficient
Training	necessary	necessary to a limited extent	necessary	necessary to a limited extent
Documentation	necessary	necessary	necessary	necessary
risk-adequate monitoring	necessary	clarification of transactions	necessary	clarification of transactions

If there is no long-term business relationship according to Article 2(1)(c) SPG, the creation of a business profile according to Article 8 SPG in conjunction with Article 20 SPV and the risk-appropriate monitoring according to Article 9 SPG may be waived. However, the contracting partner and the beneficial owner must always be identified and verified on a risk basis. In addition, the occasional transaction must always be clarified (especially with regard to purpose, background of the assets).

10. Notification of commencement of activity (Article 3(3) SPG)

Entities subject to due diligence according to Article 3(1)(u) SPG, which include persons who trade in works of art or act as intermediaries in the trade in works of art, must notify the FMA immediately in writing of the commencement of their activity (Article 3(3)(k) SPG). Notification must be sent to the FMA within five working days (postage date) of the commencement of activity. For the purposes of sending notification, the FMA provides the Notification of commencement of activities relevant to due diligence form on its website.

Persons who trade in works of art or act as intermediaries in the trade in works of art (Article 3(1)(u) SPG)

1. Group of addressees (Article 3(1)(u) SPG)

The provisions of this Special Part are addressed to persons who trade in works of art or act as intermediaries in this context and also include art galleries and auction houses within the scope of the aforementioned activity. However, due diligence only arises if the value of the transaction amounts to CHF 10,000.00 or more. But this is irrespective of whether the transaction is made in a single operation or in several operations between which there appears to be a link.

2. Territorial scope

Based on the principle of territoriality see General Part, Section 4), Liechtenstein due diligence law does not impose any restrictions with regard to the location of the assets. Consequently, the activities enumerated under Section 2 are always subject to due diligence if they are performed in and/or from Liechtenstein, regardless of whether the work of art is situated abroad.

3. Scope and application of due diligence obligations

The person subject to due diligence shall in principle comply with all due diligence obligations. The duties of due diligence (in the narrower sense) according to Article 5(1) SPG are:

- the determination and verification of the contracting partner's identity (Article 6 SPG);
- the determination and verification of the beneficial owner's identity (Article 7 of the SPG);
- the creation of a business profile (Article 8 SPG); and
- the risk-appropriate monitoring of the business relationship (Article 9 SPG).

Any reporting obligations within the meaning of Article 17 SPG remain intact.

4. Professional specifics

Since the trade in art itself is internationally considered a risky area, intermediaries in this field are therefore classified as so-called "gatekeepers". Due to their direct contact with clients, they are able to make a better risk assessment than the financial institutions that ultimately process the related payment.

Due diligence for this professional group arises whether or not there is a power of disposition over the assets of third parties and not only when they themselves provide a settlement account, receive funds on a fiduciary basis or are otherwise directly involved in the settlement of payments. Thus, pure brokerage, in which buyer and seller are brought together, is also subject to due diligence.

When acquiring or selling works of art, both the buyer and the seller must be identified as contracting partners and verified on a risk basis.

When acquiring or selling works of art, the beneficial owners on both the buying and the selling side must be identified and verified on a risk basis.

In addition, information on the origin of the assets and the background of the total assets must be determined and recorded on a risk basis.

Persons who hold third-party assets in safe custody on a professional basis and rent out premises and containers for the safekeeping of valuables (Article 3(1)(v) SPG)

1. Group of addressees (Article 3(1)(v) SPG)

Persons who hold third-party assets in safe custody on a professional basis and rent out premises and containers for the safekeeping of valuables are subject to due diligence according to Article 3(1)(v) SPG. Hereinafter they are also referred to as "custodians and lessors for the safekeeping of valuables". In principle, Article 3(1)(v) SPG is intended to cover, in particular, the activities of the storage business (bonded warehouses and valuables storage) as well as locker rental and/or management, which are carried out on the basis of a business licence issued by the Office of Economic Affairs (e.g. highly secured lockers as well as professionally secured self-storage boxes).

2. Delimitation

The following activities are not subject to this provision:

1. The safe custody of objects in lockers in publicly accessible places that can be seen from all sides (e.g. as at swimming pools or train stations).
2. The safe custody of goods such as luggage, household items, and motor vehicles.
3. The occasional safe custody of goods, to a limited extent, such as the provision of hotel safes.
4. The safe custody of non-physical objects, such as computer data.
5. The safe custody of objects in the context of the performance of security transports and other transports.
6. The renting out of commercial and industrial space.

3. Distinction between safe custody and renting

The new due diligence category fundamentally distinguishes between renting and safe custody and can be described as follows:

Holding third-party assets in safe custody:

- Activities of the storage business (bonded warehouses and valuables storage),
- Holding third-party assets safe custody in safes and vaults (depending on the form of the contract).

Renting out of containers for the safekeeping of objects:

- Locker management services:
- Renting out of safes and vaults (depending on the form of the contract).

Safe custody is the holding (storage) of third-party assets for a fee. In particular, this must be understood as more than the mere provision of premises. A safekeeping and protective activity is provided with regard to the objects brought in (cf. Article 958 of the Liechtenstein General Civil Code (*Allgemeines bürgerliches Gesetzbuch*; hereinafter referred to as the "ABGB")). With regard to safes and vaults, it will have to be decided on a case-by-case basis – depending on the form of the contract – whether this involves safe custody or the mere renting out of a container.

4. Territorial scope

Based on the principle of territoriality see General Part, Section 4), Liechtenstein due diligence law does not impose any restrictions with regard to the location of the assets. Consequently, the activities enumerated under Section 3 are always subject to due diligence if they are performed in and/or from Liechtenstein.

5. Scope and application of due diligence obligations

The due diligence obligations differ within the due diligence category according to Article 3(1)(v) SPG depending on the type of business activity and must be performed as follows:

Due diligence to be performed **Custodians and lessors for the safekeeping of valuables**		
	Renting	**Safe custody**
Due diligence in a narrower sense		
The determination and verification of the contracting partner's (CP) identity	x	x
The determination and verification of the beneficial owner's (BO) identity	x	x
Creation of business profile	* See the explanation.	x
Risk-appropriate monitoring	* See the explanation.	x
Suspicious activity report according to Article 17 SPG to the SFIU	x	x
Due diligence in a broader sense		
Logging of access	x	x
Keeping and updating the inventory list		x
Preparation of risk assessment	x	x
Check regarding PEP and media monitoring	x	x
Annual SPG report	x	x
Documentation and internal organisation	x	x

An overview of due diligence to be performed in the narrower and broader sense is given below. The explanations on these topics in this Guideline apply accordingly.

Due diligence in a narrower sense to be performed:

- The determination and verification of the contracting partner's identity (Article 6 SPG):
  In both cases, the identity of the contracting partner must be determined, verified and documented (Article 6 SPG).
- The determination and verification of the beneficial owner's identity (Article 7 SPG):
  In both cases, the identity of the beneficial owner must be determined, verified and documented (Article 7 SPG).

- The creation of a business profile (Article 8 SPG):

  In the case of safe custody, a business profile must be established including the origin of the total assets and the origin of the funds used (source of funds/source of wealth) (Article 8 SPG). This recording of source of funds/source of wealth does not apply to rentals. However, there must also be certain minimum requirements for rentals (such as knowledge and documentation of the purpose of the business relationship).

- Risk-appropriate monitoring of the business relationship (Article 9 SPG)

  Risk-appropriate monitoring of the business relationship must be done during safe custody and, as far as possible, also in connection with rentals. However, since in the case of rentals (e.g. locker) the person subject to due diligence does not have to draw up an inventory, no traditional transaction monitoring is required in this case. However, the person subject to due diligence shall nevertheless make simple and special clarifications, if necessary, both in the case of rentals and in the case of safe custody (cf. General Part, Section 5.5).

- Reporting obligations within the meaning of Article 17 SPG:
  The obligation to notify the Stabsstelle Financial Intelligence Unit according to Article 17 SPG exists in both cases.

Due diligence in a broader sense to be performed:

- Logging of access
  Access to the custody account/locker/vault and the like must be recorded in both cases with regard to the external persons present at the time of access and the time of access. The person subject to due diligence shall record those persons who are granted access. With regard to persons acting on behalf of the contracting partner, the person subject to due diligence shall ensure that the identity of such persons is established and verified by consulting a confirmatory document (cf. Article 6(3) SPV).

- Keeping and updating the inventory list
  An inventory to be kept up to date must be drawn up only in connection with safe custody. This requirement does not apply to rentals.

- Preparation of risk assessment
  The risk assessment of the business relationships must be carried out for rentals and safe custody. Reference is made also in this regard to FMA Guidelines 2013/01.

- Check regarding PEP and media monitoring
  The PEP check as well as media monitoring see General Part, Section 5.5.3) must be carried out for rentals and safe custody.

- Annual SPG report
  The persons subject to due diligence shall submit certain SPG reporting factors to the FMA on an annual basis for both rentals and safe custody (General Part, Section 14).

- Documentation and internal organisation
  The further due diligence obligations regarding documentation and internal organisation (General Part, Section 11) apply to both rentals and safe custody (keeping and retaining due diligence files, drawing up internal directives, designating internal functions, etc.)

6. Notification of commencement of activity (Article 3(3) SPG)

Persons subject to due diligence according to Article 3(1)(v) SPG, i.e. custodians and lessors for the safekeeping of valuables, shall immediately notify the FMA in writing of the commencement of their activities (Article 3(3)(l) SPG). The notification must be submitted to the FMA at the latest within five working days after

the commencement of the activity (postmark). To submit the notification, the FMA provides on its website a form: Notification of the commencement of an activity subject to due diligence.

According to Article 3(3) SPG, persons subject to due diligence according to Article 3(1)(v) SPG are only subject to notification insofar as they are not already subject to due diligence supervision by the FMA on the basis of an authorisation under a special law and the service in question is covered by this authorisation.

If persons subject to due diligence according to Article 3(3) SPG who hold a relevant licence under the Business Act terminate their activities completely, this must be reported to the FMA in writing immediately.

III. Amendments

On 7 May 2019, the following adjustments were made:

General part

- **Point 5.3.: Identification and verification of the identity of the beneficial owner and the recipients of a distribution**

  At the beginning, clarifications have been included which explain the two steps into which the identification and verification of the identity of the beneficial owner are divided.

  In addition, an adjustment was made to clearly state that the identity of the beneficial owner must be verified in any case by means of risk-based and adequate measures. Only in the case of a low risk can the collection of documents with probative value be dispensed with.

  With regard to verification of beneficial ownership itself, the guidance has been adjusted to the effect that, in the case of normal risks, the written declaration of the contracting party is not sufficient as a verification measure. In cases of normal, increased, or high risks, further measures to verify beneficial ownership are required in any case. For the purpose of explaining these measures, various documents are now given as examples or reference is made to the alternative of conducting one's own research by analogy with the explanations in FMA Guideline 2013/1.

  It has also been clarified that the guidance in the Special Part on service providers for legal entities pertaining to the identification and verification of the identity of the distribution recipients applies exclusively to that professional category under the conditions set out in Article 7a(2) and (4) SPG.

- **Point 5.5.2.: Simple and special investigations**

  Clarifications have been included concerning the elimination of unclarified fact patterns and suspicions. In this context, reference is now also made to the case law of the Constitutional Court, which defines the threshold for the offence of money laundering.

  Reference is now also made to the current case law of the Court of Appeal in connection with the submission of suspicious activity reports and of the Court of Justice in connection with the performance of special investigations.

- **Point 8.1.: Delegation**

  Guidance has been added to clarify the concept of the "other person subject to due diligence". In addition, comprehensive guidance has been included which serves to describe in detail the requirements of Article 14(1)(b) SPG.

  Furthermore, the Instruction now contains supplemental guidance on the exercise of due diligence by a "third party", which the delegation designates as such.

- **Point 8.2.: Outsourcing**

  With regard to verification of the conditions under Article 14(1) SPG, a reference has now been added to the analogous application of the guidance on delegation.

- **Point 11.2.3.: Internal functions**

It has been clarified that the responsible member of the executive body must have an in-depth knowledge in matters of the prevention and combating of money laundering, predicate offences of money laundering, organised crime and terrorist financing as well as data protection law.

In addition, the Instruction now also contains guidance on the requirements for appointing a specialised unit for the functions of compliance officer or investigating officer.

Comprehensive guidance has also been added on the separate exercise of the functions of compliance officer and investigating officer. The same has been done for substitution of internal functions. A figure has been integrated to illustrate this comprehensive guidance.

Additional guidance has also been included regarding the notification to the FMA of the appointment and change of function holders (including a deadline of five working days).

Special Part on undertakings for collective investment

- **Point 2.: Duty to update business profile**

  The 30-day time period for updating has been changed to "monthly", and the addition has been included that each business relationship must be recorded.

Special Part on insurance intermediaries

- **Point 1.: Addressees/scope**

  In order to use the wording of the Insurance Distribution Act, editorial adjustments have been made to the activities.

- **Point 2.: Due diligence obligations**

  With regard to risk-appropriate monitoring under Article 9(1) SPG, a formal adjustment has been made to clarify that monitoring of transactions performed in the course of the business relationship must be carried out, but only insofar as it is possible for the insurance broker to do so.

Special Part on asset management companies

- **Point 5.: Financial analysis**

  Guidance has been included to clarify that asset management companies do not have to perform due diligence within the scope purely of a financial analysis.

Special Part on service providers for legal entities including liquidators

- **Point 2.2.: Delimitation from lawyers, law firms, and legal agents**

  To avoid conflicts of competence or overlaps between the supervisory powers of the FMA and the Liechtenstein Chamber of Lawyers, more detailed guidance is now provided. It has been clarified that lawyers are subject to the due diligence supervision of the Liechtenstein Chamber of Lawyers when performing activities as service providers for legal entities permitted under their licence.

It has also been noted that the provisions on the provision of joint services within the meaning of Article 15 SPG do not apply under certain circumstances.

- **Point 4.1.: General remarks**

  With regard to the company- and group-internal exercise of due diligence, additional guidance has been included regarding non-mandatory compliance with the requirements of Article 15 SPG. It has also been clarified that the exemption from punishment under Article 31(8) SPG does not apply in such cases.

- **Point 4.2.: Identification and verification of the identity of the distribution recipient**

  With regard to the verification of the identity of the distribution recipient, the Instruction now contains guidance according to which a document with probative value as referred to in Article 7 SPV must be obtained.

- **Point 4.3.: Provision of joint services**

  Guidance has been included to clarify the distinction between paragraphs 1 and 2 of Article 15 SPG.

  Comprehensive guidance has also been included to clearly govern the situation when the person subject to due diligence holding the mandate leaves the group of persons subject to due diligence and the situation when a mandate is taken over.

  It is also again pointed out that the provisions on the provision of joint services may under certain circumstances not apply between persons supervised by the Liechtenstein Chamber of Lawyers and persons supervised by the FMA.

- **Point 5.2.: Service as governing body for the account of third parties**

  Due to numerous enquiries to the FMA on the subject of the protector and the protector's duty of due diligence, guidance has been included for the purpose of legal certainty which is in line with the FMA's long-standing interpretation and practice.

Special Part on casinos

This Special Part is entirely new and has been integrated into the Instruction.

Special Part on members of tax consultancy professions and external bookkeepers

- **Point 4.: Scope and application of due diligence**

  Analogous to the guidance under point 4.1 in the Special Part on service providers for legal entities, guidance on company- and group-internal performance of due diligence has been included.

Special Part on persons trading in goods

- **Point 1.: Addressees**

  It has been clarified that the provision of services such as consultancy services does not fall within the scope of Article 3(1)(q) SPG.

On 27 December 2019, the following adjustments were made:

General Part

- **Introductory text box**

  Inclusion of Article 21(2) SPV.

- **Point 5.4.:**

  Clarification regarding electronic business profiles.

- **Point 6.:**

  Editorial adjustment in the reference.

- **Point 8.1.:**

  Editorial adjustment, referring to EU Anti-Money Laundering Directive instead of 4th AMLD.

- **Point 11.2.3.:**

  Editorial adjustment in the reference.

- **Point 15.:**

  Change of entry into force of the amendments.

Special Part

- **Persons trading in goods**

  Inclusion of cash payment with virtual currencies or tokens.

- **TT service providers and other persons subject to due diligence with a nexus to TT services**

  Newly included.

On 12 March 2020, the following adjustments were made:

I. General Part

- **Point 5.2.**

  Reference to Section IV Annex 1 (formerly List C).

- **Point 8.1.**

  Reference to Section IV Annex 1 (formerly List C) and deletion of reference to FMA Guideline 2013/1.

II. Special Part

- **Undertakings for collective investment (Article (3)(1)(c) SPG)**

  Reference to Section IV Annex 1 (formerly List C).

IV. Annexes

- **Annex 1 to the General Part**

  Inclusion of Chapter IV Annex 1 (formerly List C).

The following changes were made on 25 August 2021:

I. General Part

- **Due diligence obligations**

  - **Section 5.3 (Determination and verification of the identity of the beneficial owner, the distribution recipients and the beneficiary of life insurance (Articles 7 et seq. SPG; Articles 11 et seq. SPV))**

    Deletion of the phrase (in the German version) “In the case of a low risk, obtaining confirmatory documents within the meaning of Article 7 SPV may be waived”.

  - **Section 5.4 (Business profile):**

    In addition to minor editorial adjustments, Chapter 5.4.2 (Timeliness of the business profile) was transferred from Guideline 2013/01 on the risk-based approach to the present Guideline.

  - **Section 5.5 (Risk-appropriate monitoring):**

Apart from minor editorial adjustments, some areas have been incorporated unchanged from Guideline 2013/01.

- **Section 5.6 (Media monitoring):**

  Some areas have been incorporated unchanged from Guideline 2013/01. In addition, details concerning media monitoring have been added.

- **Section 6 (PEP check):**

  In view of the amendment to the SPV, which will come into effect on 1 September 2021, additions have been made in connection with “known close associates”.

- **Section 11.2 (Internal organisation):**

  This chapter is supplemented and more detailed information is provided on the organisational structure and procedures as well as the inspection and monitoring measures, which are part of the procedures and strategies (internal directive).

- **Section 11.2.1 (Internal directive) and Section 11.2.2 (Training and development)**

  will be adjusted to the SPV amendment, which will come into effect on 1 September 2021.

- **Section 11.2.3**

  is expanded, and the duties related to the internal functions are described in more detail.

- **Section 13 (Due diligence checks):**

  Amendment of the chapter, as the fixed audit frequency in Article 37a SPV has been deleted. Inspections are done a risk basis.

- **Section 15 (Exercising due diligence in the transfer of funds):**

  New addition. The existing duties are explained.

- **Section 16 (Special obligations for persons subject to due diligence who are part of a group):**

  New addition. The existing duties are explained.

- **Section 17 (Special obligations of persons subject to due diligence in respect of international sanctions):**

  New addition. The existing duties are explained.

II. Special Part

The chapter on “Due diligence checks” was deleted from all relevant chapters of the Special Part, as the inspections are risk-based.

- **Undertakings for collective investment**

- **Sections 1.1, 1.2 and 3**

  have been amended.

- **Section 2**

  is a new addition.

- **Insurance companies**

  - **Section 2:**

    New sectioning has been added.

  - **Section 2.3:**

    It was established that forms C and T must be used for the determination of the beneficial owners of the beneficiary (legal entity).

  - **Section 3:**

    It was clarified that the responsibility for proper due diligence includes ensuring that there is no sub-delegation.

- **Insurance intermediaries**

  - **Section 3:**

    It has been established explicitly that sub-delegation is excluded.

- **Asset management companies**

  - **Section 3**

    has been amended.

- **Service providers for legal entities including liquidators (Article 3(1)(k) SPG)**

  - **Section 2 Group of addressees, Section 2.1**

    was amended, as Article 2(1)(t) SPG was repealed as part of the complete amendment of the Business Act.

  - **Section 2.2**

    was adapted to the SPG amendment, which entered into effect on 1 April 2021. Lawyers and law firms with a licence under the Lawyers Act and legal agents who provide activities according to Article 3(1)(k) SPG act as service providers for legal entities and are subject to supervision by the FMA. A clarification regarding the provision of joint services has been added.

  - **Section 4.3:**

Paragraph concerning the provision of joint services by persons according to Article 3(1)(m) and Article 3(1)(k) SPG has been amended.

- **Section 6:**

  The notification obligation according to Article 3(3) SPG was adapted due to the amendment of the SPG, which came into force on 1 April 2021.

- **Casinos**

  - **Section 4.6**

    In addition to editorial changes and/or clarifications, Section 4.6 was added in connection with the minimum requirements for politically exposed persons (PEPs). Specifically, it was established when a casino must perform and/or repeat a PEP check.

  - **Section 5.3.5**

    Furthermore, the systematic recording of payouts with vouchers was regulated consistently in Section 5.3.5. The casinos already spoke out in favour of recording payouts with vouchers as part of a consultation in 2020, as there is an increased risk of money laundering.

- **Members of tax consultancy professions and external bookkeepers (Article 3(1)(n) SPG)**

  - **Section 5.1**

    was formally adapted to the amendment of the SPG, which came into force on 1 April 2021. The content was not changed.

  - **Section 6**

    was supplemented and it was clarified that the obligation to report according to Article 3(3) SPG does not apply if the authorisation under a special law includes the activity of an external bookkeeper and/or tax consultant.

- **Real estate brokers (Article 3(1)(p) SPG)**

  - **Sections 1 to 3**

    This chapter was adapted to the amendment of the SPG, which came into force on 1 April 2021. Real estate brokers are now also required to exercise due diligence in connection with the rental of real estate if the monthly rent is CHF 10,000.00 or more.

  - **Section 6**

    is adapted, clarifying that reports according to Article 3(3) SPG are required by real estate brokers according to Article 3(1)(p) SPG regardless of whether they are already subject to due diligence supervision by the FMA on the basis of a special law authorisation.

- **Persons trading in goods**

  - **Section 4**

is adapted, clarifying that reports according to Article 3(3) SPG are required by persons trading in goods according to Article 3(1)(q) SPG regardless of whether they are already subject to due diligence supervision by the FMA on the basis of a special law authorisation.

- **TT service providers**
  - **Section 3.1.7**

    is a new addition (TT agent).

  - **Section 6.1**

    was supplemented. All transactions must be subjected to a sanction screening of the relevant wallet address, provided that the analysis supports the relevant TT systems.

  - **Section 6.6**

    is a new addition (correspondent banking relationships).

  - **Section 6.7**

    is a new addition (transactions to unhosted/private wallets)

  - **Section 6.8**

    is a new addition (internal transactions on a platform)

  - **Section 9**

    is a new addition (self-issues)

- **Persons who trade in works of art or act as intermediaries in the trade in works of art (Article 3(1)(u) SPG)**
  - **New addition**
- **Persons who hold third-party assets in safe custody on a professional basis and rent out premises and containers for the safekeeping of valuables (Article 3(1)(v) SPG)**
  - **New addition**

IV. Annexes

- **Annex 1**

  Third countries that have due diligence and record-keeping requirements and supervisory standards that are consistent with the requirements set out in the Anti-Money Laundering Directive (EU): United Kingdom is a new addition

On 13 April 2022, the following adjustments were made**:**

I. General Part

- **Section 5.3 Identification and verification of the identity of the beneficial owner, the recipients of a distribution and the beneficiary of life insurance (Articles 7 et seq. SPG; Articles 11 et seq. SPV)**

  The previous explanations concerning the collection of documents have been replaced by references to the new explanations under Section 5.4.2. It has also been set forth that the totality of the ownership and control structure must be documented in the due diligence files and be comprehensible to third parties (see Article 7(2) SPG).

- **Section 5.4.1 General**

  Explanations concerning the updates of the business profile were deleted from the General Part and transferred unchanged to section 5.4.3; the reference to Guideline 2013/1 was deleted without replacement.

- **Section 5.4.2 Content of the business profile with respect to source of funds (SoF) and source of wealth (SoW)**

  New addition of the section under 5.4.2.

- **Section 5.4.3 Updates of business profile**

  Formal adjustment; the section corresponds to the previous Section 5.4.2.

  Deletion of section on "Plausibility check of information and documentation" (previous Section 5.4.3). This section has become obsolete due to the new explanations in Section 5.4.2.

- **Section 5.5.2 Simple and special investigations (Article 9 SPG; Article 22 SPV)**

  The reference to Section 5.3.3 of FMA Guideline 2013/1 has been replaced by reference to Section 5.4.2 of this Instruction.

II. Special Part

Special Part for TT service providers (Article 3(1)(r) SPG) and other persons subject to due diligence with a nexus to TT services (Article 3(1)(s) and (t) SPG)

- **Section 4 Risk assessment**

  The references to FMA Guideline 2013/1 have been replaced by references to Section 5.4.2 of this Instruction.

- **Section 5 Business profile**

  The reference to FMA Guideline 2013/1 has been replaced by the reference to Section 5.4.2 of this Instruction.

IV. Annexes

Annex 1

Third countries with due diligence and safekeeping requirements and supervisory standards consistent with the requirements set out in the Anti-Money Laundering Directive

In connection with the following SPG and SPV provisions, direct or indirect reference is made to due diligence and safekeeping obligations and supervisory standards that are consistent with or correspond to the requirements set out in the EU Anti-Money Laundering Directive:

- Article 14(1)(b) SPG (delegation)
- Article 18b(3) SPG (exemption from ban on disclosure)
- Article 3(1)(g) SPV in conjunction with Article 22b(3) SPV (identification of beneficial owner)
- Article 9(b) SPV (confirmations of authenticity from other persons subject to due diligence according to Article 3(1)(a) to (i) of the Act, a lawyer, a trustee, an auditor or an asset manager)
- Article 24(4)(b) SPV (delegation within the group)
- Article 24a(1)(b)(2) SPV (outsourcing)

The FMA has examined the due diligence and safekeeping obligations and supervisory standards of the following countries and concluded that they are consistent with the requirements set out in the Anti-Money Laundering Directive with regard to financial institutions:[50]

Brazil (BR)	Israel (IL)	South Africa (ZA)
Guernsey (GG)	Japan (JP)	South Korea (KR)
Hong Kong, China (HK)	Jersey (JE)	United Kingdom (UK)
India (IN)	Switzerland* (CH)	United States of America (US)
Isle of Man* (IM)	Singapore (SG)	

For the countries marked with an asterisk (*), it can be assumed that their systems for combating money laundering and terrorist financing are consistent with the requirements of the Anti-Money Laundering Directive also with regard to non-financial institutions.[51]

The Member States of the European Economic Area (EEA) are *de jure* obliged to implement the due diligence and recordkeeping requirements laid down in the EU Anti-Money Laundering Directive and the supervisory requirements laid down in Chapter VI Section 2 of the EU Anti-Money Laundering Directive. The systems for combating money laundering and terrorist financing in the Member States of the European Economic Area (EEA) can therefore be assumed to meet the requirements of points 1 and 2 of Article 14(1)(b) SPG.

[50] Persons subject to due diligence which are banks, investment firms, undertakings for collective investment, insurance undertakings, insurance brokers, payment service providers, asset management companies, etc.

[51] Persons subject to due diligence which are service providers for legal entities, lawyers, notaries, statutory auditors, external bookkeepers, tax consultants, etc.