FMA

Finanzmarktaufsicht
Liechtenstein

FMA Instruction 2021/18 Obligations when carrying out TT transfers

Reference:	FMA Instruction 2021/18
Addressees:	Entities subject to due diligence according to Article 3(1)(r) and (t) of the DDA
Concerning:	Liechtenstein Law of 11 December 2008 on Professional Due Diligence to Combat Money Laundering, Organized Crime, and Terrorist Financing (*Gesetz vom 11. Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung, SPG* – Due Diligence Act, DDA) and the associated Due Diligence Ordinance (DDO)
Publication	FMA website
Enactment	18 August 2021
Entry into force	18 August 2021
Last amendment	–
Legal bases	Article 12a DDA Article 4 DDO Article 23(b) et seqq. DDO

Content

Landstrasse 109 • P.O. Box 279 • 9490 Vaduz • Liechtenstein
Telephone +423 236 73 73 • Fax +423 236 73 74 • www.fma-li.li • info@fma-li.li

1. Background

With the amendment to the DDA of 1 April 2021, the basis for the exchange of information concerning the data on the beneficiaries and originator of a transaction on a TT system was created in Article 12(a) of the DDA. With the amendment of the DDO of 1 June 2021, these regulations were given substance in Article 4 and 23(b) et seqq. of the DDO. These provisions will now be explained and the details set out in the following instructions.

Recommendation No. 15 of the Financial Action Task Force (FATF) recommendations states that, in the case of transfers of token or virtual currencies, similar to the provisions of the Money Transfer Regulation, an exchange of information regarding the data of the beneficiary and the originator should be carried out between TT service providers. This explanation is fundamentally based on the Money Transfer Regulation and the requirements of FATF Recommendation No. 16.

2. Scope of application

According to Article 23(b) of the DDO, an exchange of information is required for all transfers of tokens or virtual currencies (tokens) that currently exceed the amount of CHF 1.00. The rule applies in principle to all entities subject to due diligence according to Article 3(1)(r) and (t) of the DDA (TT service providers)[1].

The deciding factor in the obligation to exchange information is whether the token is actually transferred. This means that a transfer in some form takes place on the TT system with which the TT service provider is involved. Ultimately, this means that a TT service provider who initiates, carries out, executes or orders a transfer of a token on the TT system[2] is obliged to carry out an exchange of information if a TT service provider is also involved on the opposite side, and the amount to be transferred exceeds CHF 1.00.

If the counterparty (instructing or benefiting TT service provider with whom a TT transfer is concluded) is a foreign service provider who, if registered in Liechtenstein, was a TT service provider subject to registration under the Liechtenstein TVTG, there is also an obligation to carry out an exchange of information. In this case it is possible that the service provider abroad is a registered payment service provider or a bank. An exchange of information must also be carried out if the foreign service provider is subject to the application of the “travel rule” due to its activities abroad.

2.1. Exceptions

Token issuers are exempt from this obligation if the transfer is carried out as part of the initial offering. If further transfers are carried out beyond this (secondary market), however, token issuers also fall within the scope of the travel rule provisions.

If TT transfers are carried out on a white-label platform, these TT transfers are also excluded from the scope of application of the travel rule, as in principle a central operator of the white-label platform is already required to obtain and verify all data and information on users within the framework of KYC rules in advance.

TT agents are exempt from this obligation to the extent that the obligations are assumed by the foreign TT service provider for whom they distribute or perform the services.

[1] In an unspent transaction output (UTXO) system, a transfer is considered to be the transfer from one TT Identifier to another, irrespective of the number of transactions, whereby transaction fees and “change outputs” may be disregarded.

[2] In the case of a TT service provider that commissions a transfer by a sub-custodian, the TT service provider is obliged to exchange information, and not the sub-custodian. Delegation to the sub-custodian is permitted, however.

Intermediary service providers (routing, clearance, operation of a lightning node, etc.) are exempted from the obligation to forward information to the extent that this is not necessary for the exchange of information between the TT service providers.

3. Determining the counterparty

In order to carry out the exchange of information, it must be established whether or not the counterparty is a beneficiary TT service provider (possibly an originating TT service provider). This determination of the counterparty is thus relevant for any transfer of tokens with an equivalent value of more than CHF 1.00.

The legislator stipulates that a counterparty determination must be made before a TT transfer is completed, but leaves it open in which way this is to be carried out. The TT transfer is considered to have been completed once the beneficiary or the originator can freely dispose of the transferred tokens. If the transferred tokens remain blocked in the beneficiary's account, for example, the TT transfer has not yet been completed.

Various procedures can be used to determine the counterparty. On the one hand, it can be done through the use of a standard that, for example, involves maintaining a central VASP register or by verifying the counterparty by means of a smart contract. On the other hand, the counterparty can be determined provisionally, for example, by assigning the TT identifier to a specific counterparty with a high degree of probability using a blockchain tracking tool, or by notifying the originator or beneficiary of a specific counterparty. The latter is particularly relevant if the standards developed cannot yet be implemented or applied appropriately.

Trusted central VASP registers are those registers that are maintained by supervisory authorities or other international or supranational organisations. In principle, registers that are kept by service providers in connection with travel rule implementation applications, and for which these service providers also verify the persons entered in the register, are also considered trustworthy.

Once a beneficiary TT service provider (or, if applicable, an originating TT service provider) has been determined as a counterparty, it must also be verified. In doing so, access must be gained to the register of the competent supervisory authority, or the counterparty must be verified through comparison with other publicly available and trustworthy registers. If necessary, verification can also be carried out by means of reconciliation via the information transmitted. This is generally done automatically when using a standard.

Once the verification has been completed, the way in which information is to be transmitted will be agreed with this counterparty.

4. Exchange of information

Information must be exchanged in a secure manner prior to the completion of the TT transfer. "In a secure manner" means that the route of transmission must be secured according to the current state of the art. If a standard is used to transmit the information[3], it can basically be assumed that the transmission is secure. In principle, information can also be exchanged without the use of a standard.

4.1. Collection of information by the originating TT service provider

The following information must be collected by the originating TT service provider prior to the exchange of information:

- name (first and last names/company name) of the beneficiary and the originator;
- the designation or number of the TT account (e.g. the TT identifier) of the originator and the beneficiary; and

[3] The Travel Rule Protocol (TRP) or OpenVASP, for example.

- the address, the number of a valid official identity document, the customer number or the date and place of birth of the originator.

Prior to the exchange of information, the originating TT service provider is required to implement measures and policies to ensure that all information regarding the originator is verified, accurate and transferable. As a rule, this information is found in the client's business profile, and is recorded and verified when the business relationship is established.

With regard to operators of physical money-changing machines, which are only subject to due diligence according to Article 5(2)(h) of the DDA above a threshold value of CHF 1,000.00, the obligation to determine and verify in connection with the exchange of information also applies above a threshold value of CHF 1.00. This means that a limited KYC obligation starts from a threshold value of just CHF 1.00.

Furthermore, the originating TT service provider will implement measures and strategies to ensure that information on the beneficiary has been obtained, and that it is also transferable and not meaningless, whereby the information on the beneficiary is not to be verified.

Finally, the TT transfer may only be carried out, or initiated by the originating TT service provider, once all of the information relevant for carrying out the exchange of information is available.

4.2. Sanction screening by the originating TT service provider

In addition to the verification of the originator's data, the originating TT service provider is also obliged to carry out sanction screening. This is to be carried out in principle for the information on both the originator and the beneficiary. In addition to the TT account, the name of the originator and beneficiary must also be matched.

4.3. Obtaining the information from the beneficiary TT service provider

The beneficiary TT service provider will obtain and verify the beneficiary information. As a rule, this is done as part of the onboarding/KYC process when starting the business relationship with the beneficiary.

4.4. Sanction screening by the beneficiary TT service provider

In addition to verifying the beneficiary's data, the beneficiary TT service provider is also required to carry out sanction screening. This is to be carried out in principle for both the originator and the beneficiary information. In addition to the TT account, a name check must also be carried out.

Sanction screening must take place before the TT transfer is completed.

4.5. Plausibility check of the information from the beneficiary TT service provider

Once the information has been transmitted, the beneficiary TT service provider will check the relevant information for completeness. In addition to this, the plausibility check must also include an analysis of the accuracy and meaningfulness of the data. It must be checked, for example, that a name has actually been entered in the name field and not a random string of characters or even meaningless information such as "my client". Under "TT identifier of the originator", for example, it must be checked whether this is actually an address of the relevant TT system.

Subsequently, the beneficiary TT service provider must verify the correctness of the beneficiary information transmitted by comparing it with the beneficiary information it has obtained and verified itself.

The information transmitted must be verified before the TT transfer is completed. The tokens must not be made available to the beneficiary until all information is correct and complete, and the sanction check was negative.

4.5.1. Incomplete or non-transmitted information

The beneficiary TT service provider must implement effective procedures and strategies to determine whether the information has not been transmitted, or has been transmitted incompletely. Such effective procedures enable an incomplete or missing transmission to be detected, and prevent the TT transfer from being completed. If information is missing or incomplete, the first step is to request a correction/improvement from the originating TT service provider within three working days. If the originating TT service provider does not meet this deadline, the TT transfer must be rejected or returned. If the TT transfer cannot be rejected, it may be necessary to re-transfer the tokens.

4.5.2. Meaningless and incorrect information

The beneficiary TT service provider must implement effective procedures and strategies to determine whether the transmission of information was incorrect or meaningless. Such procedures are considered effective when meaningless or incorrect information can be detected and the TT transfer can be prevented in such cases. If a TT identifier should consist of 27 to 34 alphanumeric characters, for example, but only 26 characters are included in the transmission, the information is incorrect. If the information is meaningless, the first step is to request that the originating TT service provider provide the correct information within three working days. If the originating TT service provider does not comply with this request, the TT transfer will be rejected. If the information is incorrect, a simple clarification as per Article 9(3) of the DDA must be carried out. Within the framework of the simple clarification, a further exchange of information on the matter can take place with the originating TT service provider or, for example, a repetition of the determination and verification of the identity of the contracting party and the beneficial owner. If the simple clarification does not lead to a full resolution, a suspicious activity report must be sent to the Stabsstelle Financial Intelligence Unit (SFIU) and the assets temporarily frozen.

4.5.3. Information transmitted late

The beneficiary TT service provider must implement effective procedures and strategies to determine whether the information is transmitted late. If the information is transmitted late, the beneficiary TT service provider can request the originating TT service provider to transmit the information without delay. The beneficiary TT service provider may automatically reject or refuse the TT transfer or carry out a re-transfer.

5. Measures with regard to TT service providers repeatedly failing to comply

In the context of information transmission, entities subject to due diligence must provide strategies and procedures in cases where the other TT service provider repeatedly fails to comply, fails to transmit the information at all or transmits incomplete, meaningless or incorrect information. In order to be able to determine whether a TT service provider repeatedly fails to comply, procedures must be in place that allow individual incorrect transmissions of information to be attributed to a TT service provider. It is also necessary to determine which criteria are to be applied in assuming failure to comply. This can be done, for example, on the basis of a certain percentage of all transactions, or an absolute value. It is also relevant whether the other TT service provider is cooperative when it comes to clarifications.

If a TT service provider is found to have repeatedly failed to comply, further measures must be taken. Depending on the severity of the breach, various escalation levels can be applied. This may include conducting or repeating due diligence on the counterparty (see section 6), a warning, a temporary or complete ban on further TT transfers or, in cases where the counterparty is already subject to a travel rule requirement in its country of domicile, notification of the competent supervisory authority in the country (FMA). Such notification will involve transmitting all documents relating to the TT transfers, the breaches and the counterparty itself.

6. Verifying the counterparty

If a TT transfer is concluded multiple times with a counterparty in a high-risk country (money laundering or terrorist financing), these counterparties must be subjected to in-depth monitoring in order to reduce the risk of TT transfers related to money laundering or terrorist financing. Counterparty verification is carried out in the same way as for correspondent bank relationships[4], and should always be done with the approval of senior management. In addition to verifying whether the counterparty is subject to supervision, the verification should focus on assessing the risk exposure in terms of the counterparty's relation to predicate offences using a blockchain tracking tool and an adequate KYC process. Reference can also be made to independent, reliable sources. In addition, the counterparty should also be subject to due diligence at regular risk-based intervals, which includes the risk exposure with regard to the reference to predicate offences and a media search, the quality of the information exchange as well as direct questioning – for example the Wolfsberg Questionnaire[5].

The risk-based approach to repeating due diligence is based in particular on the quality of the information exchange and the findings regarding adverse media.

High geographical risks exist in particular if the counterparty is registered in a Tier 1 to 3 country according to the Global Terrorism Index[6] or a country with strategic deficits according to Annex 4 of the DDO[7].

If the counterparty poses a high or increased risk, TT transfers are subject to enhanced due diligence requirements. This is reflected by both the enhanced verification and monitoring of the counterparty and by the more in-depth clarification of the TT transfer. The latter can be done, for example, by the counterparty transmitting the KYC information.

7. Measures for transfers that are not subject to the travel rule

If a TT transfer is not subject to the travel rule because the counterparty is not a TT service provider or foreign equivalent, enhanced due diligence requirements apply to this transaction. Regardless of any other classification of the business relationship, measures must be taken to reduce the risk associated with the lack of verification of the counterparty. The entities subject to due diligence must therefore implement appropriate procedures and strategies to reduce risks. Methods of risk reduction can include, for example, the collection and verification of third-party documents that can be used to check the purpose and volume of the transfer, or a proof of ownership in the case of a transfer to or from the client's unhosted/private wallet. In addition to this, such transactions must in any case be analysed using a blockchain tracking tool.

8. Documentation

All documents assigned to the transactions must be stored in the due diligence file, with a record being kept in particular of all measures taken. In addition to the transaction data, the information on the originator and the beneficiary, the counterparty and its registered office, as well as all measures taken and clarifications made in connection with sections 4, 5 and 7 of this Instruction must also be documented.

With regard to annual reporting, the transaction data must be filed in such a way that the transaction volume and the registered office of the counterparty can be evaluated.

If there is frequent correspondence with a counterparty, the measures taken to verify the counterparty must be documented. The creation of a Virtual Asset Service Provider (VASP) register is recommended in this regard.

---

[4] See section 6.6 of the FMA Instruction 2018/07, chapter II TT service providers.

[5] www.wolfsberg-principles.com/wolfsbergcb.

[6] www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf.

[7] www.gesetze.li/konso/2009.98.

9. Internal instructions

The strategies and procedures, as well as the related processes in connection with the requirements of the travel rule, must be included in the internal instructions for entities subject to due diligence.

10. The "Sunrise problem"

In connection with the global implementation of the travel rule, different approaches are being pursued in regulation and there are also significant differences in the progress made with this regulation[8]. Some countries have already fully implemented the travel rule in their legal requirements and some countries have additionally provided for far-reaching transition periods, while many have not yet specified any regulations in this context.

Irrespective of the standard discussion or the problem of determining the counterparty, the different legal requirements worldwide make it difficult for entities subject to due diligence to actively implement the travel rule requirements. Large foreign TT service providers may not be obliged to exchange information, for example, but domestic TT service providers dependent on them may be. Given that implementation involves significant effort, in such cases the foreign TT service provider is unlikely to be motivated to implement the exchange of information, and ultimately it will be difficult for the domestic dependent TT service provider to comply with the information exchange requirements.

In this regard, the domestic TT service provider should take a risk-based approach as follows:

First and foremost, an attempt should be made to exchange information. If this is rejected by the counterparty, this must be documented. A corresponding risk assessment must then be carried out as described in section 8 of this Instruction. If the counterparty has its registered office in countries with a fundamentally high ML/TF risk, appropriate measures must be taken to reduce the transfer risk. If the counterparty originates from the European Union (EU)/European Economic Area (EEA) area or an equivalent third country within the meaning of Annex 1 of FMA Instruction 2018/07, a TT transfer without exchange of information may be concluded up until 1 April 2022 at the latest. For counterparties from all other jurisdictions, a TT transfer without information exchange may be concluded until 31 December 2021 at the latest. For all TT transfers in which this risk-based approach is taken, enhanced due diligence and appropriate risk reduction measures must be applied. Irrespective of this, all requirements (with the exception of information exchange) must be complied with. The strategies and procedures regarding the risk-based approach must be stipulated in the internal instructions.

This risk-based approach does not apply to counterparties in countries that already require full implementation of the travel rule. An exchange of information must always be carried out with counterparties from such countries.

11. Data protection

The content of these Instructions does not affect the provisions of data protection legislation. Entities subject to due diligence must therefore always comply with the requirements of data protection – in particular the European General Data Protection Regulation (GDPR) 2016/679 – when implementing these Instructions.

[8] See also the "Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs": www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html.

12. Final provisions

12.1. Entry into force

The FMA Instruction will enter into force on 18 August 2021.

Last updated: 18 August 2021