Transfer of Funds Regulation (TFR)

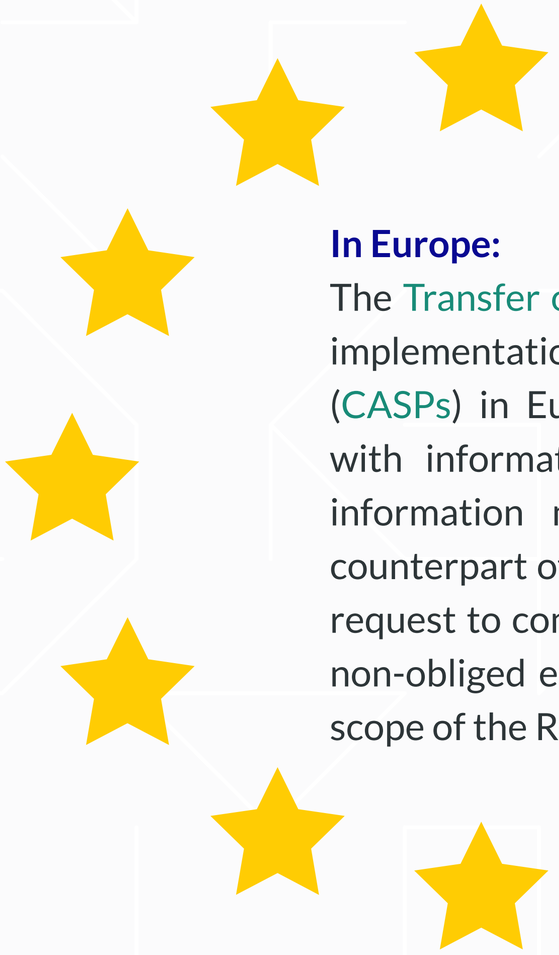
Travel Rule Regulation Guide European Union

21 ANALYTICS

20 April 2023

What Is the Travel Rule?

The Travel Rule is Financial Action Task Force's (FATF's) Recommendation 16. It requires companies transacting crypto assets on behalf of their clients to collect, store and exchange information on the originator and beneficiary involved in the transaction.



In Europe:

The Transfer of Funds Regulation* (TFR) is the European Union's implementation of the Travel Rule. Crypto asset service providers (CASPs) in Europe must accompany transfers of virtual assets with information on their originators and beneficiaries. This information must be obtained, held, and shared with the counterpart of the virtual asset transfer and must be available on request to competent authorities. Transfers involving CASPs and non-obliged entities (like self-hosted wallets) are also under the scope of the Regulation with specific requirements.

*The Regulation is also officially titled: Regulation on information accompanying transfers of funds and certain crypto-assets (recast)

Who Must Comply?

The obliged entities are crypto asset service providers (CASPs) registered in the European Union. They must comply when transferring crypto assets on behalf of their customers.

Designed to be applied together and in accordance with the Markets in Crypto Assets (MiCA) Regulation, the TFR applies to CASPs as defined by MiCA Article 3(1), point (15):

The TFR also applies to intermediaries: businesses that are not the originator's or beneficiary's CASP but receive and transmit a transfer of crypto assets on behalf of one of these CASPs.

The custody and administration of crypto assets on behalf of third parties

The operation of a trading platform for crypto assets

The exchange of crypto assets for fiat currency that is legal tender

The exchange of crypto assets for other crypto assets

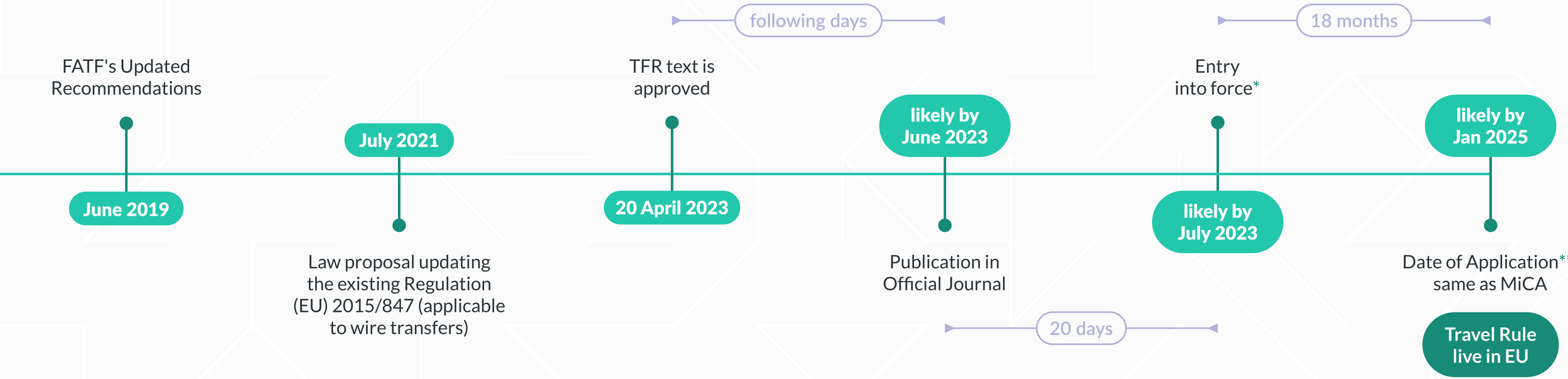
The execution of orders for crypto assets on behalf of third parties

The placing of crypto assets

The reception and transmission of orders for crypto assets on behalf of third parties

Providing advice on crypto assets

Timeline



* Entry into force means the law exists and is valid in the European Union. It is also when the grace periods start.

** Date of Application is when the Regulation becomes binding throughout the EU.

Threshold

EUR 0

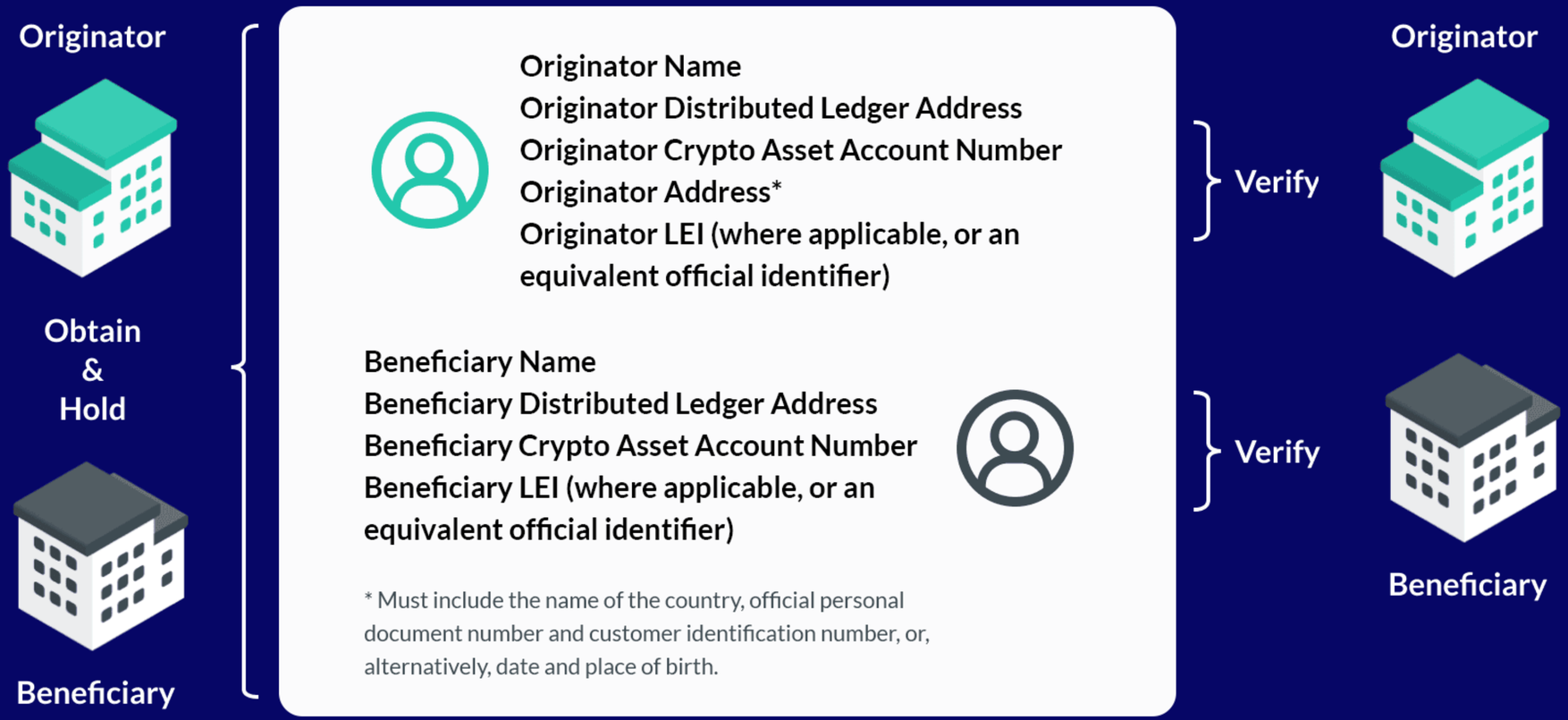
Every crypto asset transfer between obliged entities must fulfil the TFR's data collection, storage and exchange obligations with the counterparty.

What changed

Previous versions of the text allowed the collection, storage and exchange of fewer data for transfers up to EUR 1000 between European CASPs (domestic transfers). However, due to the borderless nature of crypto, the approved text now demands that all crypto-assets transfers be subject to the same requirements regardless of their amount and whether they are domestic or cross-border.

Information Required

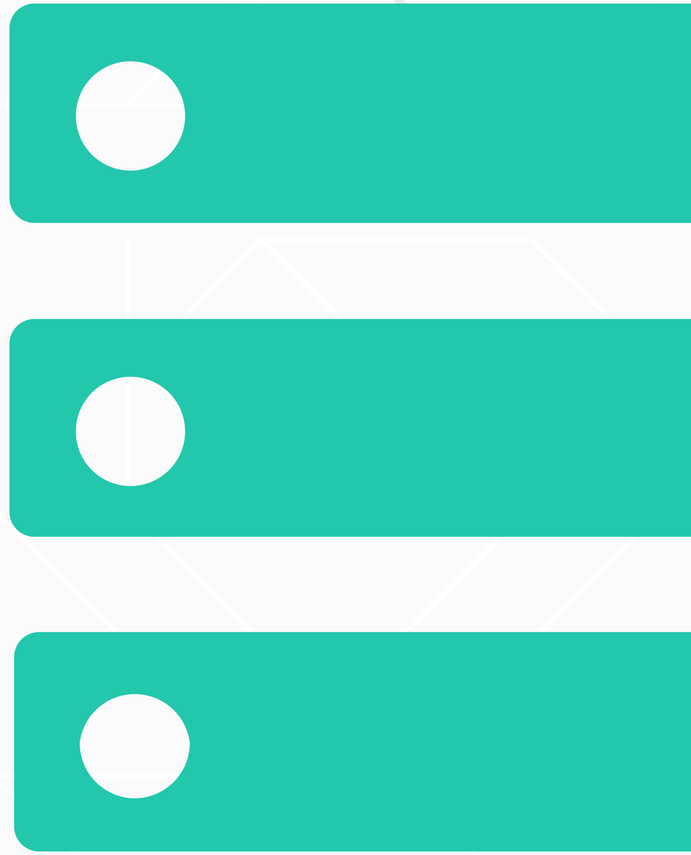
The originating CASP must ensure that transfers of crypto assets are accompanied by the following required data:



Data Sharing

The information required must be submitted in advance of, or simultaneously with, the transfer of crypto assets, in a secure manner and in accordance with GDPR.

The originator CASP shall not allow for the initiation, or execute any transfer of crypto assets before ensuring full compliance.



Missing Data

CASPs must guarantee, through established effective procedures, that the information required by the TFR is not missing or incomplete.

The beneficiary CASP must implement effective risk-based procedures to determine whether to execute, reject, return or suspend a transfer lacking information and to take the appropriate follow-up action.

Coming up

The European Banking Authority (EBA) should issue guidelines on how CASPs can detect cases in which they receive transfers of crypto assets with missing or incomplete information.

Data Protection

The processing of personal data under this Regulation should take place in full compliance with the GDPR.

CASPs shall ensure at all times that the transmission of any personal data on the parties involved in a transfer of funds or a transfer of crypto assets is conducted in accordance with the GDPR.

CASPs should put appropriate measures in place to protect personal data against accidental loss, alteration, or unauthorised disclosure.

Coming up

The European Data Protection Board should, after consulting the EBA, issue guidelines on the practical implementation of data protection requirements for transfers of personal data to third countries in the context of transfers of crypto assets.

Know-Your-Counterparty

CASPs must perform Enhanced Due Diligence (EDD) to assess and identify AML/CTF risks, similar to that applied in the context of banking when establishing a new relationship with another CASP, specifically the ones outside the European Union.

When transferring crypto assets on behalf of a client to a CASP outside of the EU, the originating CASP should assess the ability of the beneficiary CASP to receive and retain the information required in accordance with the GDPR.

Self-hosted Wallets

Self-hosted wallets are not obliged entities. Therefore, peer-to-peer transactions (from a self-hosted wallet to a self-hosted wallet) are not in scope.

However, the requirements always apply when there is a CASP involved. In the case of a transfer to or from a self-hosted address, the CASP should collect, usually from its client, and hold, but not verify, the information on both the originator and the beneficiary. The CASP must also ensure that the transfer can be individually identified.

Attention

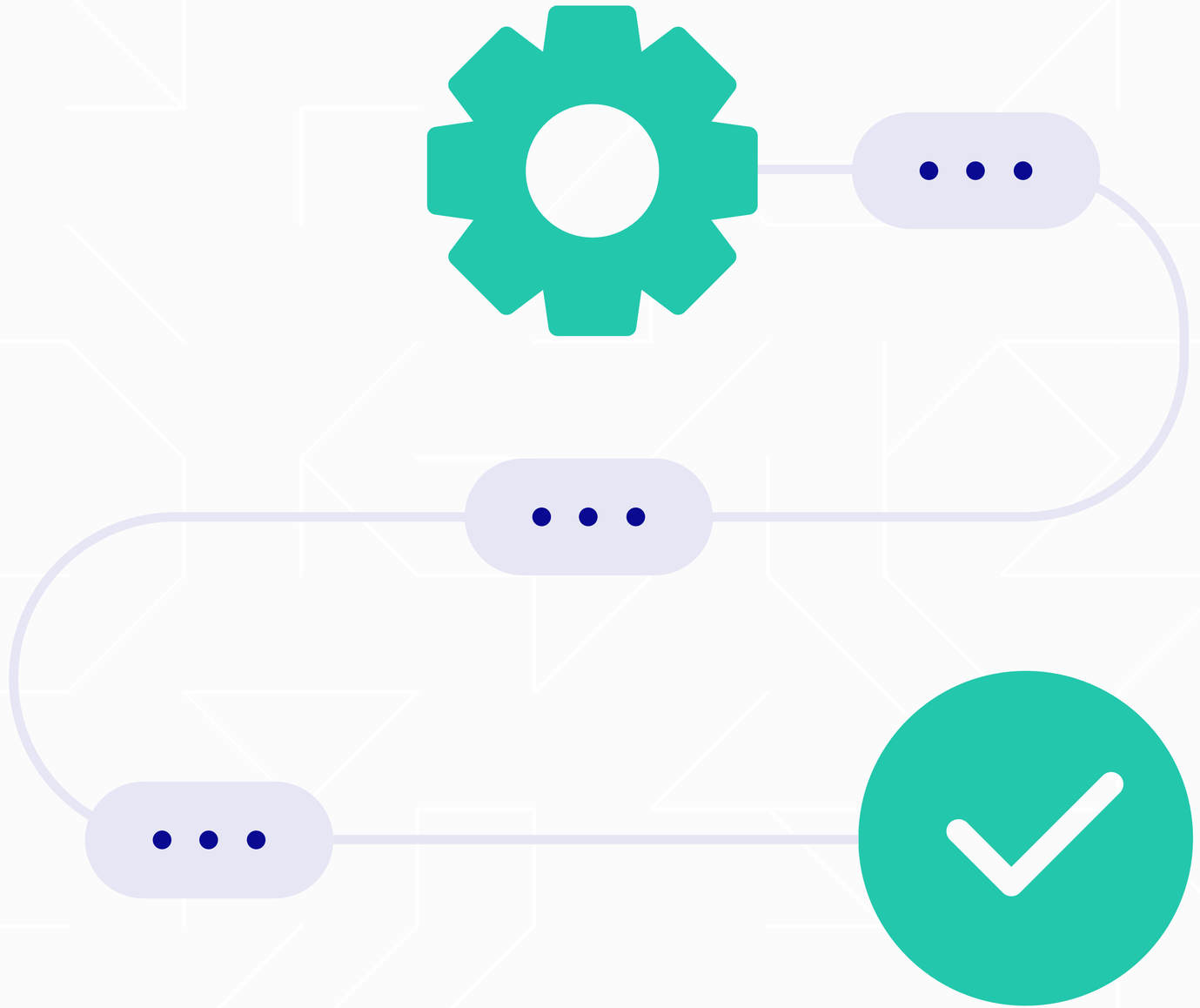
For transfers above EUR 1000 that involve a self-hosted wallet and a CASP, CASPs should verify whether the self-hosted address is effectively owned (or controlled) by their client.

What Next?

The Travel Rule is taking shape around the world and will be a requirement for CASPs in the European Union.

Although there is still no industry consensus on the protocols for data transfer, it is highly recommended that CASPs choose open and peer-to-peer protocols, following Bitcoin's initial design. This, not only enables privacy as required by this regulation, but also allows for flexibility in connecting to a broader network of counterparty CASPs.

Check out TRP to learn more about the industry's only **free and decentralized** Travel Rule protocol.



About the Author

21 Analytics provides privacy-first Travel Rule compliance software. None of your data is shared with us. Founded by Bitcoiners who have been working in the blockchain industry since 2014, 21 Analytics leverages its experience to advance our idea of combining compliance with data protection and strengthening privacy for financial intermediaries and their customers.

21 Analytics AG
Zug, Switzerland

info@21analytics.ch
www.21analytics.ch

Request a Demo

21 ANALYTICS