www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, version 4 June 2026

T-CY (2026)2

Cybercrime Convention Committee (T-CY)

Mapping study on virtual assets and the relevance of the Convention on Cybercrime and its Second Protocol

Adopted by the 34th Plenary of the T-CY on 4 June 2026

Document prepared by the T-CY Bureau

Contents

Contact

Secretariat of the Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Email T-CY.secretariat@coe.int
www.coe.int

Abbreviations

AFP	Australian Federal Police
AML	Anti-Money Laundering
BC	Budapest Convention
CASPs	Crypto asset service providers
CC	Criminal Code
CCP	Code of Criminal Procedure
CDD	Customer due diligence
CFT	Countering the Financing of Terrorism
CPC	Criminal Procedure Code
C-PROC	Cybercrime Programme Office of the Council of Europe
DCCP	Dutch Code of Criminal Procedure
DIICOT	Directorate for Investigating Organized Crime and Terrorism
ECHR	European Convention on Human Rights
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
GWG	German Money Laundering Act
ISPs	Internet service providers
KYC	Know your customer
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MoU	Memorandum of understanding
NFTs	Non-fungible tokens
PSAN	Prestataires de services sur actifs numériques
StPO	Strafprozeßordnung (Code of Criminal Procedure)
TFR	Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849
TIA Act	Telecommunications (Interception and Access) Act 1979
T-CY	Cybercrime Convention Committee
VAITOS	Virtual Asset and Initial Token Offering Act 2021
VAs	Virtual assets
VASP	Virtual asset service provider

1 Introduction

The criminal use of virtual assets (VAs) has emerged as a significant challenge for criminal justice authorities, including with respect to cybercrime, electronic evidence and international co-operation. This raises important questions regarding the applicability and practical use of the Convention on Cybercrime (Budapest Convention) and its Second Additional Protocol.

The 30th Plenary Meeting of the T-CY (June 2024), therefore, decided:

- To invite the T-CY Bureau to present the T-CY Plenary with possible options for future work of the T-CY on the question of VAs and the relevance of the Convention on Cybercrime and its Second Protocol for criminal investigations, the collection of evidence, the search, seizure and confiscation of assets, and the co-operation with virtual asset service providers (VASPs) related to offences involving VAs.

- To invite the T-CY Secretariat and C-PROC to undertake preparatory work in this respect, such as a mapping of current practices, that may assist the T-CY Bureau.

The 31st T-CY Plenary (December 2024) adopted a questionnaire to seek information from Parties to facilitate the preparation of the present mapping study. T-CY members were invited to prepare consolidated replies in coordination with competent national authorities, including authorities responsible for the implementation of the FATF Recommendations [1]. In total, 44[2] replies were received from Parties and observers.

The work on VAs also builds on the T-CY Assessment Report on Article 19 of the Convention (search and seizure of stored computer data) [3], adopted at the 31st Plenary in December 2024. The report encouraged Parties to establish clearer guidance for national authorities on the application of procedural powers in specific practical situations, including those that may arise in relation to VAs.

The 32nd T-CY Plenary (June 2025) invited the T-CY Bureau and Secretariat to prepare – in co-operation with the Cybercrime Programme Office of the Council of Europe (C-PROC) – a draft mapping study on VAs and the relevance of the Convention on Cybercrime and its Second Protocol for consideration by T-CY 34 (mid-2026).

A dedicated workshop held during the Octopus Conference on 5 June 2025 further underscored the importance of enhanced cross-border co-operation between criminal justice authorities, financial intelligence units and VASPs, and confirmed the value of examining how existing treaty tools may be applied more effectively in cases involving virtual assets[4]. The Conference

[1] See FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 2012-2025.

[2] Replies from the following jurisdictions were received by the T-CY Secretariat (by 27 February 2026): Albania, Andorra, Armenia, Australia, Brazil, Bulgaria, Canada, Costa Rica, Czechia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Ireland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Montenegro, Morocco, Netherlands, Norway, Peru, Philippines, Poland, Portugal, North Macedonia, Romania, Serbia, Sierra Leone, Slovakia, Spain, Sri Lanka, Switzerland, Tunisia, Türkyie, United States.

[3] T-CY Assessment Report: Assessing Article 19 Budapest Convention on the search and seizure of stored computer data, adopted by the 31st T-CY Plenary of the T-CY on 12 December 2024.

[4] See the Key take-aways from the Octopus Conference 2025.

has therefore greatly welcomed the ongoing mapping exercise undertaken by the T-CY to examine the applicability of the Convention to VAs and VASPs.

The 33rd T-CY Plenary (November 2025) took note of the update on a draft mapping study. It also adopted the T-CY Workplan for 2026-27, which identifies the completion of the mapping study as one of its objectives[5].

The present study was prepared by the T-CY Bureau based on a preliminary analysis carried out by the T-CY Secretariat and C-PROC. The findings draw primarily on consolidated replies to the questionnaire.

The study maps current practices among Parties and observers relating to VAs and examines the relevance and application of the Convention on Cybercrime and its Second Additional Protocol.

Its aim is also to inform the T-CY on options for future work, including possible guidance to Parties.

The study was adopted by the 34th T-CY Plenary on 4 June 2026.

2 Definitions and concepts

2.1 Virtual assets as “computer data”, “property”, or both

Question 1 of the questionnaire asked whether VAs (such as cryptocurrencies, non-fungible tokens, gaming tokens and governance tokens) are defined in domestic criminal law or case law and, if so, whether they are considered to constitute “computer data”[6], “property”, both, or another legal category.

The question was to clarify how VAs are legally characterised at domestic level and how such characterisation may interact with the procedural framework of the Budapest Convention. In particular, the qualification of VAs may be relevant when assessing whether measures of the Convention relating to computer data apply:

- only to computer data held, controlled or accessible through VASPs[7] (excluding the VAs themselves), or
- also to the VAs as such.

This distinction may have practical implications for the possible use of measures such as preservation, search or seizure directed at VAs, as opposed to the use of procedural powers limited to other VASP-held computer data relating to those assets.

---

[5] T-CY Workplan for the period January 2026 – December 2027, adopted by the 33rd T-CY Plenary on 13-14 November 2025, objective 4.2.

[6] Under Art. 1.b of the Budapest Convention "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

[7] For example, identification data, including name, date of birth, address, contact details, account creation data, wallet addresses, transaction histories or other technical metadata, including IP addresses, login timestamps other than virtual assets as such.

2.1.1 Overview of approaches

The replies indicate that most jurisdictions do not define VAs (such as cryptocurrencies, NFTs, gaming tokens, and governance tokens) expressly in domestic criminal law.

Out of 44 responding countries:

- 20 jurisdictions[8] indicated that VAs are defined outside the criminal law framework (typically in regulatory, supervisory or AML/CFT legislation) and approached primarily as property/assets or related economic interest concepts.
- 1 jurisdiction[9] indicated that VAs are defined outside the criminal law framework (in the financial regulatory framework) and are explicitly recognised as both computer data and property/assets.
- 11 jurisdictions[10] reported that, while not defined in criminal law, VAs may be treated in practice as both computer data and property/assets.
- 1 jurisdiction[11] reported treatment in practice primarily as computer data.
- 1 jurisdiction[12] reported explicit recognition in criminal law as both computer data and property/assets.
- 1 jurisdiction[13] reported recognition as property rights rather than property.
- 5 jurisdictions[14] reported explicit treatment as property/assets in criminal law or through case law.
- 4 jurisdictions[15] reported no definition in criminal law and no clear alternative classification yet or legislation under development.

These responses demonstrate that more countries rely on property or asset-based concepts, often derived from regulatory or AML/CFT frameworks[16]. At the same time, several replies describe VAs being recorded, transferred or otherwise processed electronically within computer systems, and in some cases explicitly refer to their treatment as computer data. Some jurisdictions explicitly refer to a dual understanding in which VAs may be treated as property/assets while also being addressed as computer data (or treated as such in practice).

---

[8] Albania, Andorra, Costa Rica, France, Iceland, Ireland, Israel, Latvia, Liechtenstein, Lithuania, Mauritius, Montenegro, North Macedonia, Peru, Sierra Leone, Spain, Sri Lanka, Switzerland, Tunisia, Türkiye.

[9] Japan.

[10] Australia, Czechia, Fiji, Finland, Georgia, Germany, Hungary, Norway, Philippines, Poland, Serbia.

[11] Portugal.

[12] Romania.

[13] Netherlands.

[14] Brazil, Canada, Moldova, Slovakia, United States.

[15] Armenia, Bulgaria, Ghana, Morocco.

[16] For the use of virtual assets in the AML/CFT context see MONEYVAL, Money Laundering and Terrorist Financing Risks in the World of Virtual Assets. Typologies report, 2023 and MONEYVAL, Practice of Using Virtual Assets, Virtual Asset Service Providers in the Laundering of Criminal Property, Financing of Terrorism, and the Evasion of Sanctions. Typologies report, 2025.

Other replies distinguish between the VAs themselves and computer data relating to those assets (for example, records, "bookkeeping" or transactional information), which may be treated as computer data even where the asset is primarily approached as property. The replies, therefore, suggest that domestic classifications do not follow a single model and may vary depending on the legal context.

The fact that VAs may rather be treated as property or assets under domestic law does not necessarily exclude their qualification as "computer data" within the meaning of the Budapest Convention. Conversely, recognition of their computer data-based character does not preclude their treatment as property or assets for other legal purposes.

2.1.2 Selected examples

The replies to the questionnaire contain several illustrative examples of how VAs are characterised in domestic legal systems.

- Australia reported that while VAs are not specifically characterised as "computer data", their digital nature is recognised in investigative contexts. Certain types of VAs may fall within broad statutory definitions of "communications" or data under telecommunications legislation and may also fall within the definition of "computer data" of the Budapest Convention.

- In Brazil, Law 14.478/2022 regulates VAs, which are considered property and subject to AML/CFT rules. At the same time, the bookkeeping or registration of VAs transactions is considered "computer data" within the meaning of the Convention, reflecting a distinction between the VAs itself and its related digital records.

- In Canada, case law has clarified that VAs may constitute intangible property, notwithstanding the absence of a specific statutory definition in the CC. Some courts have rejected the argument that seizure of cryptocurrency itself provides information (or evidence) about an offence in the context of particular warrant applications.

- Czechia recognises the dual nature of VAs. It noted that VAs could fall within the definition of "computer data" under the Convention. However, it was pointed out that provisions relating to "stored computer data" (notably Article 16) would apply only partially, as VAs are stored in wallets accessible only to their holder, which may limit the ability of VASPs to preserve the assets themselves as stored computer data.

- In Finland, the Criminal Code or criminal procedure acts such as the Coercive Measures Act do not define virtual assets separately. VAs or crypto-assets are assessed in the crime investigation as data or property. Where coercive measures are targeted on crypto-assets for their monetary value they are assessed mainly as property.

- AML/CFT law on VAs in Hungary is based on the recently approved Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto-assets (MiCA[17]). Article 3.1(5) of MiCA defines crypto-asset as "a digital representation of a

[17] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology". This regulation is also applicable in other EU m/S. In criminal procedure, the concept of "electronic data used for making payments" may also be of relevance.

- Japan and Romania reported that VAs may be recognised both as assets of economic value and as data recorded and processed within computer systems, explicitly acknowledging their dual character.

- Mauritius stated that VAs are covered by the Virtual Asset and Initial Token Offering Act 2021 (VAITOS) and are considered to be properties and also data, as they are "digital representation".

- In the Netherlands, VAs are described as "property rights" rather than property in the strict civil law sense. This distinction reflects domestic doctrinal considerations while allowing criminal law measures to apply to the economic interest represented by the asset. In 2024, the Dutch Supreme Court ruled that bitcoin qualifies as "property" within the meaning of specific money laundering provisions of the Penal Code, confirming its susceptibility to confiscation. The ruling concerned bitcoins specifically, literature is strongly divided on how VAs should be qualified.

- In Norway, there is no formal definition of VAs, but the courts have applied existing functional definitions, that may develop with case law over time, drawing on historic analogies (e.g. electricity as intangible property). Norwegian courts have ordered seizure and confiscation of cryptocurrency in practice.

- Peru specified that VAs are not expressly defined in criminal law. However, the domestic law does include sectoral regulations for the prevention of money laundering and CFT. Any assets that constitute the object, instrument, effects or proceeds of illegal activities, including the so-called VAs are assets subject to seizure by the state.

- By contrast, Portugal indicated that VAs are treated primarily as computer data in practice, highlighting an emphasis on the data-based dimension.

- In Sierra Leone, VAs are defined in the AML act as "a digital representation of value that can be digitally traded, transferred or used for payment or investment purposes but does not include digital representation of fiat currencies, securities, and other financial assets''.

- Spain referred to Supreme Court case law (e.g. STS 326/2019), recognising bitcoin as an intangible asset of patrimonial value capable of forming the object of criminal offences, while distinguishing it from legal tender.

2.2 VASPs and the concept of "service provider" under the Budapest Convention

Question 2 of the questionnaire asked whether VASPs (e.g. cryptocurrency businesses, crypto-asset exchange providers, non-fungible token trading sites, crypto-ATM operators and wallet custodians) are defined in domestic law and, if so, whether they are considered "service providers" under Article 1.c of the Budapest Convention.

Such qualification may affect the possible use of certain procedural measures specifically providing for co-operation with service providers, including Article 18.1.b of the Convention and Article 7 of the Second Additional Protocol.

Most other procedural powers under the Convention do not refer exclusively to "service providers". Measures that are not limited to service providers may, where appropriate, remain applicable in the VASP context, irrespective of how such entities are characterised under domestic law.

2.2.1 Overview of approaches

The replies indicate that most jurisdictions do not define VASPs in criminal law, but that many jurisdictions do define and regulate VASPs in domestic law outside the criminal law framework, typically through AML/CFT and/or financial market legislation.

On the basis of the replies of 44 reporting countries:

- 37 jurisdictions[18] reported definitions and/or regulation of VASPs in AML/CFT, supervisory or financial regulatory frameworks.

In these jurisdictions, VASPs are typically defined through activity-based descriptions (e.g. exchange, transfer, safekeeping, administration, or operation of trading platforms) and are subject to registration, licensing or AML obligations.

- 6 jurisdictions[19] indicated either that VASPs are not defined, not regulated, or that no specific legislative framework is currently in place. In several of those countries, legislative reforms are under way or being considered.

None of the replies indicated that VASPs are defined in criminal codes as a distinct and autonomous criminal law category. This, however, does not imply that criminal law measures cannot apply in relation to VASPs. In many jurisdictions, service providers are defined and regulated under sector-specific legislation (for example legislation on electronic communication services) rather than in criminal codes. The location of the definition in regulatory law, therefore, does not seem to determine whether criminal law measures may apply.

The key question, therefore, seems not to be solely where VASPs are defined in domestic law, but whether their functions may bring them within the scope of the concept of "service provider" under the Budapest Convention.

[18] Albania, Andorra, Australia, Brazil, Canada, Czechia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Ireland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Montenegro, North Macedonia, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Sierra Leone, Slovakia, Spain, Switzerland, Türkiye, United States.

[19] Armenia, Bulgaria, Costa Rica, Morocco, Sri Lanka, Tunisia.

2.2.2 Relevance for the definition of "service provider" under the Budapest Convention

A number of jurisdictions[20] explicitly addressed whether VASPs qualify as "service providers" within the meaning of Article 1.c of the Budapest Convention[21].

Other jurisdictions, such as the United States, adopted a more qualified approach, indicating that VASPs are generally not considered "service providers" within the meaning of Article 1.c, except to the extent that they perform the functions identified in that provision. Czechia similarly noted that there is no explicit rule, and that qualification may depend on the concrete services offered, including whether the provider enables online communication through its systems.

Several jurisdictions[22] explicitly indicated that VASPs do not qualify as "service providers" within the definition of Article 1.c. The Netherlands also noted that the emphasis of VASPs lies primarily on facilitating services that do not necessarily constitute communication services only, suggesting a more nuanced view of their qualification under the Convention definition.

In a number of replies[23], VASPs were described as "service providers" under domestic regulatory frameworks without an explicit assessment of whether this corresponds to the Convention definition. In these cases, the terminology used in domestic legislation may overlap with the Convention concept, although the link to Article 1.c was not expressly analysed.

A significant number of jurisdictions (approximately 40%) did not explicitly address whether VASPs qualify as "service providers" within the meaning of Article 1.c, even where VASPs are defined or regulated domestically. This may also suggest that the qualification of VASPs as service providers within the meaning of Article 1.c remains under consideration by the authorities in some jurisdictions.

Overall, the replies reflect three approaches: explicit inclusion of VASPs within Article 1.c.; activity-based or case-by-case assessment depending on the functions performed by VASPs; or exclusion based on a restrictive reading of the definition provided under Article 1.c. In many cases, the relationship between VASPs and Article 1.c was not expressly examined.

2.2.3 Selected examples

The replies provide several illustrative approaches:

- Australia noted that VASPs are addressed through multiple legislative instruments (notably AML/CTF), illustrating a framework where the concept is developed through

[20] Examples include Albania, Australia, Brazil, Georgia, Germany and the Philippines which expressly indicated that VASPs fall within the Convention definition.

[21] According to Art. 1.c of the Budapest Convention c "service provider" means:
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

[22] Iceland, Japan, Moldova, Slovakia, Switzerland.

[23] Examples include Mauritius, Poland, Portugal and Serbia.

regulation. The domestic law provides for definitions of Digital Currency Exchange Providers (DCEPs), registered VASPs or digital currency exchange.

- Costa Rica explicitly indicated the absence of a specific legislative framework and that VASPs are not regulated, while noting that draft legislation was considered. Nevertheless, in practice, the services offered by such companies are accessible in Costa Rica.

- France referred to the *"prestataires de services sur actifs numériques"* (PSAN) framework (Law PACTE and the Monetary and Financial Code), listing regulated activities such as custody, exchange, and operation of trading platforms.

- Georgia specified that while there is no definition of VASPs under criminal law, Georgian courts have regularly invoked procedural powers relevant for ISPs under the Budapest Convention in respect of such entities.

- Germany referred to the definition of crypto asset service providers (CASPs) as defined in domestic law implementing the MiCA Regulation.

- Japan expressly indicated that crypto-asset exchange service providers do not qualify as "service providers" under Article 1.c, as they do not provide communication services or process/store computer data on behalf of users of such services.

- In Morocco, current national regulations do not include definitions for VASPs. However, a draft law has been introduced which defines crypto asset service providers.

- Romania reports that VASPs are expressly recognised and regulated through national AML legislation (including amendments aligned with FATF requirements).

- In Sierra Leone, VASPs are considered service providers under the AML Act 2024. They can register and obtain a license before the commencement of operations.

- Switzerland indicated that VASPs are not considered service providers within the meaning of Article 1.c, as their primary function is to enable transactions rather than to provide communication services.

- In the United States individuals and entities that offer money transmitting services involving VAs, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of VAs, are considered "money services businesses" (MSBs). VASPs are generally not "service providers" as defined in Article 1.c. of the Convention on Cybercrime, except to the extent that VASPs perform the functions identified in this article.

2.3 AML/CFT regulation of VASPs and implementation of FATF Recommendation 15

Question 3 of the questionnaire asked whether VASPs are subject to AML/CFT regulations[24], whether all categories of VASPs as defined by the FATF are covered, and whether the requirements of FATF Recommendation 15[25] have been implemented with respect to VASPs[26].

This question was included to obtain an overview of the regulatory framework applicable to VASPs at domestic level.

The existence and scope of AML/CFT obligations may be relevant in the context of the Budapest Convention insofar as such frameworks typically require VASPs to collect, verify and retain certain categories of customer and transactional information (including travel rule information for transfers). This may affect the practical availability of information that could be sought through procedural measures under the Budapest Convention and is without prejudice to the interpretation of the Convention's own definitions and powers.

2.3.1 Overview of approaches

The replies indicate that AML/CFT regulation of VASPs is now widespread among responding jurisdictions, typically through designation of VASPs (or CASPs) as obliged/reporting entities, with accompanying registration/licensing, customer due diligence, record-keeping and in many jurisdictions travel rule requirements.

At the same time, the level of implementation of FATF Recommendation 15 varies. Several jurisdictions reported full or largely compliant implementation and broad coverage of FATF VASP categories. Others reported partial implementation or gaps, most commonly relating to the coverage of all FATF-defined activities (including issuer-related services), the scope of licensing/registration regimes, supervisory reach (including over natural persons), or the operationalisation of travel rule requirements, sometimes reflected in MONEYVAL/FATF technical compliance ratings.

A further group of jurisdictions reported ongoing reforms or transitional arrangements, including reforms expected to take effect in 2026 and, in the EU context, the entry into force of the MiCA and TFR regulations[27].

---

[24] In 2019, FATF extended the scope of AML/CFT measures to cover VA and VASPs. See FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, 2025.

[25] Recommendation 15 extends the broader FATF requirements to VASPs, including but not limited to record keeping obligations (Recommendation 15 and indirectly Recommendations 10 and 11) and 'travel rule' that applies the payment transparency requirements (FATF Recommendation 15 and indirectly Recommendation 16 The travel rule requires VASPs and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when transferring VAs).

[26] See for example, the Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity: VACG ROADMAP: JURISDICTIONS WITH MATERIALLY IMPORTANT VIRTUAL ASSET ACTIVITY (fatf-gafi.org).

[27] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

A minority of jurisdictions report that VASPs are not yet subject to AML/CFT regulation or that Recommendation 15 has not been implemented. Legislative developments are under way in several of these countries.

A small number reported prohibition models (for example, where VA-related activity is prohibited domestically). The replies nevertheless suggest that such approaches do not eliminate the practical relevance of VAs for domestic authorities, including in cross-border situations. In some of these jurisdictions, legislative developments are considered.

2.3.2 Selected examples

- Australia: AML/CTF rules currently focus on fiat–digital currency exchange; legislative amendments adopted in 2024 will expand coverage to capture the FATF-required services, taking effect 31 March 2026.

- Brazil: AML/CFT compliance for VASPs is addressed through Resolutions No. 519, 520 and 521 of the Central Bank of Brazil, issued on 10 November 2025 and in force since 2 February 2026, which establish a comprehensive regulatory regime for Virtual Asset Service Provider Companies and include .

- Canada: VASPs are regulated as (domestic and foreign) money services businesses under AML/CFT law; Canada reported implementation of FATF Recommendation 15 and broad coverage of VASP activities, including applicability to wallets/private keys where a financial service is offered.

- Costa Rica: VASPs are not currently regulated under AML/CFT law. However, a draft legislation has previously been considered.

- Czechia: VASP categories are treated as obliged entities under domestic AML law (including both MiCA-defined CASPs and other VASPs), subject to supervision; the reply indicated that FATF Recommendation 15 requirements are met.

- Fiji: Trade/investment in VAs is prohibited, and VASPs are therefore not subject to an AML/CFT regime at present; discussions on an appropriate regulatory framework are under way.

- France: Digital asset service providers (PSANs) are subject to mandatory registration (for specified services) and AML/CFT compliance checks as part of the registration process, including risk assessment and CDD obligations aligned with FATF requirements.

- Germany: CASPs and VASPs are obliged entities pursuant to Section 2.1 No. 2 of the German Money Laundering Act (GwG), with travel rule compliance deriving from direct application of the TFR Regulation, alongside MiCA authorisation requirements.

- Ghana: The reply describes draft and policy work on VA regulation; banks and payment service providers remain prohibited from facilitating crypto-asset transactions pending formal regulatory guidelines.

- Japan: Applies AML/CFT obligations to crypto-asset exchange providers under the Act on Prevention of Transfer of Criminal Proceeds.

- Mauritius: Applies AML/CFT obligations to VASPs under financial services regulation.
- Peru: VASPs are subject to AML/CFT regulations under SBS Resolution No. 02648-2024, which the reply indicates covers FATF-defined VASP categories, with FIU-Peru acting as supervisor for AML/CFT purposes.
- Philippines: AML/CFT obligations and travel rule-type requirements are implemented via central bank circulars.
- Portugal: VASPs have been obliged entities since 2020 under national AML law and Banco de Portugal supervision; since 30 December 2024 the EU TFR Regulation applies directly, while MiCA Regulation introduced an authorisation regime with a transitional period and pending designation of competent authorities in domestic implementing law.
- Sierra Leone: Reports that VASPs including all their categories are subject to AML/CFT regulations under the AML Act 2024. Reply indicates implementation or FATF Rec 15.
- Sri Lanka: Amendments to the Financial Transactions Reporting Act (FTRA) are currently being discussed.
- Switzerland: The activities of most VASPs qualify as financial intermediation and are therefore covered by the scope of AML/CFT regulations.
- United States: VASPs are regulated as money services businesses (MSBs) under FinCEN and are subject to AML/CFT obligations, including registration and suspicious activity reporting.

2.4 Subscriber information under Article 18 of the Budapest Convention in relation to VASP users

Question 4 of the questionnaire asked whether two categories of information could constitute subscriber information in the meaning of the Budapest Convention in relation to users of VASP services:

(i) customer due diligence (CDD) information under FATF Recommendation 10, and
(ii) information accompanying qualifying virtual asset transfers subject to Travel Rule requirements under FATF Recommendation 16.

While AML/CFT frameworks, including those based on FATF Recommendations, define categories of CDD and transfer-related information that VASPs are required to collect and retain, the qualification of such information as “subscriber information” under Article 18.3[28] of the Convention is assessed in light of the Convention’s own definitions.

[28] Art. 18.3 of the Budapest Convention reads as follows: 3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
a the type of communication service used, the technical provisions taken thereto and the period of service;
b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

Regulatory classifications under AML/CFT law do not in themselves determine the scope or applicability of procedural powers under the Convention. However, the existence of such obligations may affect the practical availability of information that could be sought through Convention-based measures.

2.4.1 Overview of approaches

The replies show a broad range of approaches:

- 23 jurisdictions[29] indicated that both categories (CDD information under FATF Rec. 10 and transfer-related information under FATF Rec. 16) could constitute subscriber information.

- 5 jurisdictions[30] considered that information used for identification and verification of the customer and beneficial owner under FATF Recommendation 10 could constitute subscriber information.

- 5 jurisdictions[31] indicated that neither category constitutes subscriber information. The reasons for this were that VASPs are not considered as service providers within the meaning of Art. 1.c of the Budapest Convention (they do not provide to users of its service the ability to communicate by means of a computer system, but rather that of carrying out transactions) or the domestic framework lacks the definition of VASPs.

- Other jurisdictions pointed out that this question is under analysis of the domestic authorities[32] or that the domestic authorities have conflicting positions[33] and several remaining jurisdictions did not provide a reply on this point or reported no experience.

Overall, the replies suggest that a majority of responding jurisdictions accept that CDD-based identification and verification data may fall within the concept of subscriber information under Article 18.3. Greater divergence emerges in relation to transfer-related information accompanying specific transactions, particularly where such information is viewed as transactional or traffic data rather than as information linked to the subscriber relationship itself.

2.4.2 Selected examples

The following examples illustrate the approaches reflected in replies:

---

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

[29] Albania, Andorra, Armenia, Australia, Bulgaria, Costa Rica, Czechia, Fiji, France, Ghana, Hungary, Iceland, Israel, Liechtenstein, Moldova, Norway, Peru, Poland, Portugal, Romania, Serbia, Spain, Tunisia.

[30] Brazil, Finland, Georgia, Philippines, United States. Spain reported both but specified that identity/name of the beneficiary and the beneficiary account number where such an account is used to process the transaction is consider subscriber information only in cases of public transmission (such as the one made on blockchain).

[31] Japan, Netherlands, Sierra Leone, Sri Lanka, Switzerland.

[32] Canada and Germany.

[33] Slovakia.

- In Brazil CDD-related information collected under FATF Recommendation 10 may be treated as subscriber information within the meaning of Article 18.3 of the Budapest Convention. By contrast, transfer-related information under FATF Recommendation 16 (the Travel Rule) is more appropriately characterised as transactional data. A recent regulatory update in Brazil (National Monetary Council Resolution No. 5,280 of February 26, 2026) included VASPs among the institutions subject to the law on the confidentiality of financial institutions' operations (Complementary Law No. 105/2001), which requires a court order for law enforcement access to transaction data.

- Georgia pointed out that information used to identify and verify the customer and beneficial owner under FATF Recommendation 10 may constitute subscriber information. The second set of data would most probably be considered as transactional data. When requesting such data from foreign VASPs Georgian authorities usually rely on a domestic power that is equivalent of Art. 32 of the Budapest Convention.

- Germany pointed out that as far as CASPs are considered service providers within the meaning of the BC, information that leads to the identification and verification of the identity of the customer and the beneficial owner can be interpreted as subscriber information according to article 18.3 of the Budapest Convention. However, the German authorities did not provide a unanimous response to this question, and the matter therefore remains under analysis by the national authorities.

- Japan indicated "none", reflecting the view that neither CDD information nor transfer-related information constitutes subscriber information in the meaning of the Convention.

- Netherlands also indicated "none", showing that some Parties adopt a restrictive approach to the notion of subscriber information in relation to VASP users.

- Peru reported "both", pointing out to the definition of subscriber information under the BC and its ER. It explained that subscriber data includes:

  a) Identification and verification data, such as photos of the user's national ID, a photo of the user, names, email addresses, phone numbers, and the date of registration.
  b) Bank transfer data, such as information identifying financial service users, the banks involved, transaction details, and destination addresses.

  Peru further pointed out that subscriber data covers identification and verification information of both the customer and the final beneficiary. For example, when someone creates an account on a cryptocurrency exchange, the provider collects details like the person's full name, ID document, address, and proof of the final beneficiary (if acting for someone else). This information links the user to activities on the platform. Similarly, for cross-border transfers, the data attached to the transaction (such as the name, address, or date of birth of the sender and the beneficiary) is stored by the providers involved. This allows transfers to be traced back to identified individuals.

- Philippines pointed to FATF Recommendation 10 identification and verification information, illustrating a narrower approach anchored in CDD-related information.

- Poland indicated that both CDD information and transfer-related data may constitute subscriber information, noting that account identifiers for virtual currency services fall within the understanding of "account" under domestic AML law.

- Portugal indicated "both", suggesting that subscriber information may encompass both identity/verification data and transfer-related information connected to VASP services.

- Romania stated that under its domestic law, the information related to users of VASPs, including identification data, transaction details, and financial records, can be considered subscriber information as defined in the Budapest Convention.

- Slovakia reported conflicting domestic positions, illustrating that classification is not yet settled across competent authorities.

- Spain specified that CDD/KYC information constitutes subscriber information. However, it distinguished between identity data and transfer-related data. Beneficiary information linked to a specific transfer may qualify as traffic data, particularly where it results from a communication process rather than from the subscriber relationship itself.

- United States identified FATF Recommendation 10 identity and beneficial owner verification information, indicating that this category may constitute subscriber information in relation to VASP users. It would not consider the names and information relating to originators and beneficiaries for specific cross-border wire transfers to constitute subscriber information within the meaning of the Budapest Convention.

3 Use of criminal procedural powers to obtain evidence from VASPs

3.1 Application of procedural powers under the Budapest Convention in the VASP context

Question 5 of the questionnaire asked to what extent domestic authorities can apply procedural powers, similar to those provided under the Budapest Convention, for obtaining data from VASPs.

This question was included to examine whether, and how, procedural powers corresponding to Articles 16–21 of the Convention are applied in practice in relation to VASPs and VAs. It sought to identify what types of measures are used in the VASP context, whether such powers are applied to obtain data from VASPs, and whether certain measures, for example those corresponding to Article 16 and 19, are also relied upon in relation to VAs themselves.

The section therefore discusses the reported use of the Budapest Convention procedural measures in the VASP context, while broader domestic frameworks governing seizure and confiscation of VAs are examined separately in Section 3.2.

3.1.1 General overview

The replies suggest that, in most jurisdictions, there are no VASP-specific procedural rules for obtaining data. Rather, authorities apply existing procedural powers that are available in relation to persons, entities or service providers.

Jurisdictions most frequently report that they can use non-real-time measures, such as data preservation (Arts 16–17), production orders (Art 18), and search and seizure (Art 19), to obtain computer data held by VASPs other than VAs themselves.

By contrast, the use of the real-time collection of traffic data (Art. 20) and the real-time interception of content data (Art 21), is more uneven: some Parties report the powers are available, while others report “no”, “not specified”, or “yes but no practice”.

The most detailed replies also illustrate that, in practice, VASP-related evidence sought often includes CDD/KYC and account identifiers, transaction histories, logs/metadata (including IP logs), in some cases communication data and where relevant, measures to freeze/seize VAs (including transfer to law-enforcement-controlled wallets).

3.1.2 Orders for data preservation (Art. 16-17 of the Budapest Convention)

3.1.2.1 Overview of approaches

On the basis of the replies of 44 reporting countries:

- 33 jurisdictions[34] reported that preservation-type measures can be applied in relation to data associated with VASP services (other than preservation/freezing of VAs as such).
- 2 jurisdictions[35] reported that the preservation-type measures are not applied.
- Remaining 10 jurisdictions have not specified this in their reply.

The measure is used to obtain preservation of the following data: account data, transaction-related records, subscriber/KYC information, and logs (where held by VASPs) subscriber information and data concerning the bookkeeping of VAs.

At least two jurisdictions[36] explicitly reported securing VAs themselves in practice in connection with powers implementing Article 16 of the Convention. Other replies[37] indicate that, depending on national law and the way Article 16 has been implemented, domestic measures equivalent to data preservation may in practice allow authorities to secure or prevent the movement of VAs.

[34] Albania, Armenia, Australia, Brazil, Costa Rica, Czechia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Israel, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Netherlands, Norway, Philippines, Poland, Portugal, Romania, Serbia, Sierra Leone, Spain, Switzerland, Türkyie and United States.

[35] Canada, Slovakia.

[36] Czechia, Germany.

[37] Examples include Iceland, Norway, Portugal.

3.1.2.2 Selected examples

- Australia: The TIA Act (specifically, Part 3-1A) allows for the AFP to obtain the type of information referred to in Articles 16 and 17 of the Budapest Convention. Part 5-1A of the TIA Act requires a service provider covered under that Part (effectively carriers and carriage service providers) to retain certain information (generally subscriber information for that service and traffic data) for 2 years. Chapter 4 permits the disclosure of telecommunications data from carriers and carriage service providers, from which information about VAs or VASP user might be ascertained.

- Albania: Albanian authorities can issue data preservation orders to VASPs based on provisions of the CPC, which implement Art. 16 - 17 of the BC. These orders require VASPs to preserve specific data, including transaction histories, wallet addresses, and user activity logs for up to 90 days (renewable). Additionally, Law on Financial Markets based on the Distributed Ledger Technology (DLT) reinforces these powers specifically requiring VASPs to preserve data for a minimum period of five years, making it readily available upon lawful request within 72 hours.

- Brazil: preservation orders can be issued to safeguard transaction data related to crypto asset balances held on an exchange.

- Canada: preservation orders have not been relevant as of yet as the transactional data is immutable and public, and the VASP-held data has not been determined to be at risk.

- Finland: A person having data in their possession or under their control, other than a suspect may be ordered to keep it unchanged. It must be noted that if the target of the measure is a data asset value and the purpose is to secure assets for a probable seizure, the authorities can order the service provider an interim sequestration (interim seizure) or sequestration (seizure). This is not a data preservation order but a coercive measure on assets as property.

- France: in accordance with Articles 16 and 17 of the Convention, French judicial authorities may request a VASPs to prevent the deletion or modification of electronic data.

- Georgia: uses the power, however, it is less often used in respect of VASPs compared to other ISPs. VASPs usually have intensive data retention policies and it does not take long to get data disclosure from them.

- Germany: requirements of Article 16 covered with regard to the immediate securing of computer data by the rules of seizure in Sections 94 et seq. of the CPC.

- Switzerland: prosecution offices can issue data preservation orders to VASPs without requiring a court approval.

3.1.3 Production orders (Art. 18 of the Budapest Convention)

3.1.3.1 Overview of approaches

On the basis of the 44 replies:

- 34 jurisdictions[38] reported that they can use production orders (or equivalent powers) to compel data held by VASPs.
- 1 jurisdiction reported no[39].
- Remaining jurisdictions did not specify.

Types of evidence commonly requested are identity/KYC data and account identification data such as name, date of birth, address, copy of photo ID and account holder photo taken on account opening, transaction histories / transaction reports, IP logs, timestamps, and device/account access logs, or other "subscriber-type" or operational records held by VASPs.

3.1.3.2 Selected examples

- Albania pointed out that production orders allow prosecutors to require VASPs to provide customer KYC/CDD information, transaction histories, wallet addresses and balances, as well as IP addresses and login data. Law 66/2020 strengthens these powers by requiring licensed entities, through implementing regulations, to establish automated systems for responding to authorised data requests.
- Public prosecutors and police in Brazil can directly request subscriber information from telecommunications companies without a court order. Law enforcement can access subscriber information (name, ID number, tax ID, parents' names, and address) of individuals under investigation for money laundering. Telecommunications providers, banks, internet service providers, credit card companies, and electoral authorities hold these data.
- Canada reported that it recently amended the production order for financial data in the CC to clarify that this order is available to obtain information related to digital assets accounts and account holders.
- Moldova stated that the CPC does not regulate production orders. However, authorities apply provisions related to the collection of information from electronic communications service providers and the identification of subscribers or users of an electronic communications network.
- Netherlands described a broad set of domestic provisions enabling production orders to obtain stored data, explicitly including subscriber information, log files and other relevant computer data, and noted that MLA may be used where necessary.
- Portugal indicated that the procedural powers in its cybercrime law framework (including production orders) are applicable to obtain evidence from VASPs, on the understanding that information related to VA is treated as computer data in practice.
- Romania stated its prosecutors may issue an order requiring VASPs to provide

[38] Albania, Armenia, Australia, Brazil, Canada, Costa Rica, Czechia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Israel, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Netherlands, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Sierra Leone, Spain, Switzerland, Türkyie, United States.

[39] Slovakia.

transaction records, user identity data, source of funds, and wallet addresses. If a VASP refuses to comply, the prosecutor may request a court-issued order, which is aligned with Art. 18 of the Budapest Convention.

- Serbia specified that its authorities could obtain transaction and subscriber data from VASPs. Under the Law on Digital Assets, VASPs must collect, store, and share customer identification details and transaction records to comply with AML/CFT rules. Law enforcement agencies may access this information through court orders or investigative subpoenas. If an individual is suspected of being involved in a money laundering scheme using cryptocurrency, law enforcement may request transaction records from a VASP to trace the movement of funds. VASP would be required to provide the transaction history, including wallet addresses, amounts, and timestamps.

- Slovakia does not apply the measure, stating that the existing powers relate to computer data from service providers, not to financial transaction data.

- Spain referred to domestic provisions allowing authorities to request the delivery of stored data, whether subscriber, traffic or content data, which can also be used in VASP contexts.

- Switzerland indicated that prosecutors may issue production orders directly to VASPs to obtain relevant data, including subscriber information, transaction reports and KYC, without requiring court approval. Non-compliance can be addressed through search orders for the premises of VASPs.

3.1.4 Search and seizure of stored computer data (Art 19 of the Budapest Convention)

3.1.4.1 Overview of approaches regarding search and seizure of computer data associated with VASP services

On the basis of the 44 replies:

- 38 jurisdictions[40] reported that search and seizure powers can be used for stored data linked to VASP services. Armenia reported yes but lack of practice.

- 1 jurisdiction[41] reported no.

- Remaining jurisdictions did not specify.

Typical evidence obtained through this measure is stored account records, transaction records, logs, and other computer data, as well as evidence stored on devices/servers associated with VASP services.

[40] Albania, Andorra, Armenia, Australia, Brazil, Bulgaria, Canada, Costa Rica, Czechia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Netherlands, Norway, Peru, Philippines, Poland, Portugal, North Macedonia, Romania, Serbia, Sierra Leone, Spain, Switzerland, Türkyie, United States.

[41] Slovakia.

3.1.4.2 Selected examples regarding search and seizure of computer data associated with VASP services

- Finland pointed out that data that is contained in a computer, terminal equipment or another equivalent technical device or information system at the time of the search may be copied or seized.

- Japan indicated that subscriber information and transaction records may be obtained from domestic VASPs through investigative inquiry and search and seizure.

- Netherlands described the ability to search and seize computer data during criminal investigations. Investigators can search computers, servers, and other digital devices to access and seize stored data. They are also allowed to make copies of the data or decrypt it.

- Romania reported that if there are reasonable indications that a digital wallet or exchange platform contains evidence relevant to the investigation, authorities may request judicial authorization to conduct a forensic search of the system and extract relevant data. This measure applies to the seizure of cryptocurrencies and digital wallets (Article 168 CPC).

- Spain indicated that a provision on searching mass data storage would be legally possible in the context of VASP services, while also noting limited experience in that specific context.

- In Türkiye, seizure may be ordered under the CPC (including provisions on seizure of property and digital materials), complemented by enforcement and financial market legislation. In the CPC, Article 134 on search, copying and seizure of computers, computer programs and logs, procedures for the examination of digital materials are defined. In this context, the digital evidence of crypto-assets such as wallet addresses, private keys, etc. may be seized by the competent authorities for examination.

3.1.4.3 Overview of approaches regarding seizure of virtual assets based on power equivalent to Art. 19 of the Budapest Convention

Replies are more cautious and less detailed on the specific ability to seize VAs themselves (as distinct from stored data associated with VASP services) on the basis of power equivalent to Art. 19 of the Budapest Convention. A smaller group of 12 jurisdictions[42] explicitly reported "yes", while many answers were "not specified" on this narrower point.

In several replies, legislative provisions addressing seizure of digital assets were presented both as implementation of powers corresponding to Art. 19 and as part of broader domestic seizure or asset recovery frameworks. This suggests that, in some jurisdictions, legislative provisions framed domestically in terms of seizure of digital assets are considered to implement Art. 19 of the Budapest Convention, while also operating within broader frameworks governing freezing, confiscation and recovery of criminal assets. The interaction between these approaches is further examined in Section 3.2 which addresses other legal provisions and

[42] Albania, Australia, Bulgaria, Canada, Czechia, France, Georgia, Germany, Hungary, Mauritius, Romania, Serbia.

procedures applicable to VAs.

3.1.4.4 Selected examples regarding seizure of virtual assets based on power equivalent to Art. 19 of the Budapest Convention

- Canada recently established a special search warrant for digital assets, for seizure of proceeds of crime that are digital assets such as cryptocurrency. Existing restraint orders are available for digital assets. Typically, the warrant or order is accompanied by an assistance order or management order, where the VASP will be ordered to co-operate and send the funds to an identified police-controlled wallet.

- Czechia reported that where, seizing/freezing of VAs is concerned, legal basis of this practice provide provisions of the domestic law corresponding to provisions of the Budapest Convention on production orders and seizure, in connection with provisions on search. The competent authorities identify VAs concerned (identify that a person has such assets), they identify the virtual wallet and strive to obtain access. Where virtual wallets are stored with a VASP, they try to co-operate with it. If they obtain access (by means of a seed phrase, key or password), they transfer VAs concerned to their virtual wallets, i.e. to virtual wallets of the relevant police authorities or of the Office for Representing the State in Property Matters, which manages the seized VAs during the course of criminal proceedings, where authorised by the police authority (the authority responsible for management of seized VAs aims to carry out their interlocutory sale to prevent possible decrease in value of the seized VAs which are volatile).

- France pointed out that in line with Art. 19 of the Budapest Convention, Art. 706-154 of the CPC provides that a judicial police officer authorised by the competent judicial authority may seize a sum of money or digital assets held by a VASP. The seizure of digital assets is carried out without transfer, directly into the hands of a VASP for the purposes of transfer and storage at the Agency for the Management and Recovery of Seized and Confiscated Assets (AGRASC), from the date of notification of the report to the PSAN for the purposes of seizure.

- Germany described that under German criminal procedure law, the seizure of computer data and thus also of VAs is carried out by seizing the data carriers on which the data is stored. The rules of seizure in Sections 94 et seq. of the German CCP (StPO) are applicable in this respect. These allow the criminal prosecution authorities to access computer data directly and thus secure it for criminal proceedings.

- Serbia stated that its authorities can apply for search and seizure orders to obtain digital assets or other evidence stored by VASPs. This includes the power to seize digital assets in cases where they are suspected to be involved in criminal activities such as fraud, money laundering, or terrorism financing. For example, if a VASP's user is suspected of using cryptocurrency to finance terrorism, the authorities could apply for a court order to freeze the user's account and seize the assets stored on the platform. This would prevent further illicit transactions and enable law enforcement to gather evidence.

These examples demonstrate that seizure of VAs under powers corresponding to Article 19 may involve operational measures such as transfer to law enforcement-controlled wallets or co-operation with VASPs. In several jurisdictions, such measures form part of broader domestic

frameworks governing seizure, confiscation and asset recovery, which are addressed separately in Section 3.2 which discusses other legal provisions and procedures applicable to VAs.

3.1.5 Real-time collection of traffic data (Art. 20 of the Budapest Convention)

3.1.5.1 Overview of approaches

Compared with Arts 16–19, replies show greater variability:

- 28 jurisdictions[43] reported that they use the real-time collection of traffic data in relation to data associated with VASP services. Some of these indicated that the measure may be used only in the investigation of the most serious offences.
- 3 jurisdictions[44] reported "yes", but with no practical experience of using the measure.
- 4 jurisdictions[45] reported "no".
- The remaining jurisdictions did not specify.

Typical evidence obtained through this measure may include the IP addresses, timestamps, routing/connection information.

3.1.5.2 Selected examples

- Brazil pointed out that its authorities can collect real-time traffic data, including in cases involving VASPs. However, due to the decentralised and global nature of VA networks, the effectiveness of such measures may be limited. Judicial authorisation is required.
- Germany referred to domestic authorisation enabling the collection of traffic data, reflecting availability of Article 20-type measures under domestic criminal procedure law.
- Netherlands described domestic provisions allowing collection of traffic data in real time for serious crime investigations, including metadata such as IP addresses and timestamps, without accessing content of communications.
- Romania specified that its authorities may request real-time monitoring of electronic transactions or interception of electronic communications related to VAs.
- Spain pointed out that the possibility of capturing information in real-time (whether traffic data or content data) offers greater difficulties since the interception of communications is regulated in reference to interpersonal contacts. However, Art.

[43] Australia, Brazil, Costa Rica, Czechia, Fiji, Finland, France, Germany, Ghana, Hungary, Iceland, Israel, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Netherlands, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Switzerland, Türkyie, United States.

[44] Armenia, Canada, Spain.

[45] Albania, Bulgaria, Georgia, Slovakia.

588b (e) LECrim, which establishes the duty of collaboration for the purposes of such interceptions and includes service providers as obliged subjects, could be useful for this purpose. Additionally, real-time interception could be carried out through the remote registration of computer systems under Art. 588 septies LECrim. However, there is currently no practical experience with using this measure.

3.1.6 Interception of content data (Art. 21 of the Budapest Convention)

3.1.6.1 Overview of approaches

Replies again show more uneven reporting than those for Articles 16–19:

- 29 jurisdictions[46] use interception of data in relation to data associated with VASP services. Some of these indicated that the measure may be used only in the investigation of the most serious offences.
- 2 jurisdictions[47] reported "yes" with no practical experience.
- 5 jurisdictions replied[48] they do not use this power in relation to data associated with VASP services.
- The remaining jurisdictions did not specify.

Types of evidence obtained through this measure include messages/communications or account communications.

3.1.6.2 Selected examples

- Australia described that Part 5-3 of the TIA Act requires service providers to have an interception capability which Australian law enforcement agencies can use to record and collect contact data.
- Brazil reported that authorities can intercept content data, including in cases involving VASPs. Judicial authorisation is required.
- Peru stated that it does not have a specific provision exclusively addressing VASPs. However, general criminal procedural powers such as Interception and recording of communications (Article 230 of the CPC) apply.
- Philippines referred that its law enforcement authorities, upon securing a Warrant to Intercept Computer Data, are authorized to carry out any or all of the following activities: (a) listening to, (b) recording, (c) monitoring, or (d) surveillance of the content of communications, including procuring of the content of computer data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the

[46] Australia, Brazil, Costa Rica, Czechia, Fiji, Finland, France, Germany, Ghana, Hungary, Iceland, Latvia, Liechtenstein, Lithuania, Mauritius, Netherlands, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Switzerland, Türkyie, the United States.

[47] Armenia, Spain.

[48] Albania, Andorra, Bulgaria, Georgia, Slovakia.

communication is occurring.

- Serbia specified that its law enforcement can apply for authorization to intercept communications related to VASP activities if there is a suspicion of criminal activity. This includes communications such as the transfer of digital assets or interactions between users on VASP platforms. For example, if there is suspicion that a VASP platform is being used for illegal transactions (e.g., facilitating terrorist financing), the authorities could seek a court order to monitor communications between users or between a user and the VASP platform.

- Switzerland provided a useful clarification: because VASPs do not qualify as telecommunications providers under domestic law, content data held by VASPs (e.g., correspondence between VASP and client, account-login information) may be obtained through non-telecom procedural routes and can be conducted without court approval. However, the surveillance of banking transactions, including transactions made by clients with VASPs in Switzerland, likely requires court approval.

3.1.7 Disclosure of subscriber information (Article 7 of the Second Protocol to the Budapest Convention)

3.1.7.1 Overview of approaches

Replies show a mixed but generally positive picture regarding the ability to obtain subscriber information from VASPs using powers comparable to Article 7 of the Second Protocol:

- 21 jurisdictions[49] responded that subscriber information can be obtained from VASPs through domestic legal mechanisms equivalent to subscriber-information disclosure orders.

- 5 jurisdictions[50] reported that such disclosure is not currently possible or is not yet covered by the relevant procedural framework.

- Many jurisdictions did not provide a specific answer or indicated that the situation has not yet been assessed in the context of the Second Protocol[51].

Types of evidence obtained through this measure include identity information linked to the VASP account (name, date of birth, address, identification documents), account registration data, contact details (email address, phone number), IP log history associated with account access, customer due diligence / KYC information, wallet addresses linked to an account.

Several jurisdictions indicated that they are currently working to implement this power into their domestic legislation.

[49] Albania, Armenia, Australia, Brazil, Canada, Costa Rica, Finland, France, Ghana, Hungary, Latvia, Liechtenstein, Lithuania, Moldova, Netherlands, Norway, Philippines, Poland, Romania, Serbia and Spain.
[50] Czechia, Fiji, Germany, Iceland, Slovakia and the United States.
[51] Examples include Andorra, Georgia, Ireland, Israel, Japan, Mauritius, Montenegro, Peru, Portugal, Switzerland, Türkiye and others.

3.1.7.2 Selected examples

- Canada: this measure is covered by production orders. Typical data sought and obtained includes KYC data – name, date of birth, address, copy of photo ID and account holder photo taken on account opening, transaction history, IP log history, devices connecting to the account.

- Hungary: according to Section 265/A of the CPC, the prosecution and the investigating authority may request data in such a way that the requested body is asked to provide the data voluntarily, without the prospect of sanctions.

- France: Articles 100 et seq. of the CPC do not define the categories of persons who may be subject to judicial interception. On several occasions, the Court of Cassation has reiterated that the persons concerned 'who are not only those against whom there is evidence of guilt' may be wiretapped. This includes persons under investigation, but also any person who appears to have participated in the acts or who is likely to have information relating to them, including VASPs.

- Netherlands: Articles 126na and 126ng section 1 DCCP allow Dutch authorities to request subscriber information from service providers. Subscriber information includes basic identification details (e.g., name, address, and IP address).

3.2 Other domestic legal provisions and procedures for the search, seizure and confiscation of virtual assets

Question 6 of the questionnaire asked what other legal provisions and procedures are applied at domestic level for the search, seizure and confiscation of VAs, including the legal basis, seizure process, custodial management and confiscation procedures.

This question was included to examine how jurisdictions address VAs within their broader domestic asset recovery frameworks, beyond procedural powers corresponding to the Budapest Convention.

While certain measures of the Budapest Convention, such as those corresponding to Article 19, may in some jurisdictions also be used in relation to seizure of VAs themselves, many legal systems apply general confiscation, freezing and seizure regimes when securing and recovering VAs[52].

The section therefore explores how VAs are integrated into existing domestic seizure, confiscation and asset management frameworks, and how such measures operate in practice.

3.2.1 Overview of approaches

The replies indicate that, in addition to procedural powers for obtaining computer data from VASPs, jurisdictions rely extensively on broader confiscation, freezing and asset recovery frameworks when dealing with VAs. In most jurisdictions, these measures form part of general criminal law or proceeds-of-crime legislation.

[52] Many of these general regimes in Europe were established pursuant to the provisions of the Warsaw Convention (CETS No.198).

Several jurisdictions reported legislative provisions specifically addressing the seizure or confiscation of digital assets. In other jurisdictions, VAs are addressed within existing confiscation and asset recovery frameworks without legislative differentiation.

The replies also suggest that, in practice, measures aimed at securing control over VAs, including search and seizure of stored computer data enabling access to such assets or seizure of wallet devices, are complemented by freezing and confiscation frameworks addressing the economic dimension of those assets. The interaction between these measures reflects the dual technical and property-related characteristics of VAs.

3.2.2 Confiscation and freezing frameworks

A number of jurisdictions reported relying on general confiscation and asset recovery regimes to address VAs linked to criminal offences. These frameworks typically provide for:

- conviction-based confiscation,
- non-conviction-based confiscation,
- value-based confiscation, and
- provisional freezing or restraint measures.

In many jurisdictions, VAs are treated as "property" or equivalent assets within existing proceeds-of-crime legislation. For example:

- Australia applies the Proceeds of Crime Act (POCA), under which VAs fall within the definition of property. The POCA provides for conviction-based forfeiture, non-conviction-based forfeiture and value-based confiscation orders, including pecuniary penalty and unexplained wealth orders.

- Brazil indicated that confiscation of VAs is primarily governed by general criminal procedure and AML legislation, with digital assets included within the scope of financial crime enforcement through the Money Laundering Prevention Law. AML/CFT obligations enacted through Resolutions No. 519, 520 and 521 of the Central Bank of Brazil require VASPSs to implement internal controls to prevent the use of the financial system for money laundering or asset concealment, and to comply with sanctions obligations under Law No. 13,810/2019. These regulatory obligations operate in parallel with the criminal law confiscation framework.

- Germany confirmed that cryptocurrencies may be confiscated under Section 73 of the CC as proceeds of crime, as clarified by the Federal Court of Justice. Provisional seizure to secure enforcement is possible under the CPC.

- Israel reported that VAs are treated similarly to other financial or physical assets under criminal and anti-money laundering legislation, including value-based confiscation and, in certain circumstances, civil forfeiture.

- Moldova stated that confiscation of VAs is carried out under general criminal law provisions, while the Criminal Assets Recovery Agency is responsible for managing seized criminal assets, including VAs.

- In the Netherlands, the legal framework for the confiscation of VAs is primarily governed by the DCCP and the Dutch Penal Code. VAs are similarly treated to traditional assets in the context of criminal investigations. The Netherlands uses

various forms of confiscation, including object-based confiscation, value-based confiscation and extended confiscation.

- United States law enforcement may freeze, seize and forfeit VAs through criminal forfeiture (following conviction), civil judicial forfeiture (action against the property linked to a criminal offense, rather than against the wrongdoer) or administrative forfeiture. Each procedure requires the government to establish the connection between the asset and criminal activity.

Several jurisdictions also referred to provisional freezing or restraint measures designed to prevent dissipation of VAs during investigations. Such measures may involve court-issued restraint orders or freezing orders directed at custodial VASPs, ensuring that assets remain available pending confiscation proceedings.

Overall, the replies indicate that most jurisdictions integrate VAs into existing proceeds-of-crime frameworks rather than creating distinct confiscation regimes related to VAs.

3.2.3 Seizure of virtual assets and specific digital asset seizure powers

The replies reflect different legal bases relied upon to effect seizure of VAs. As discussed in Section 3.1.4, a number of jurisdictions reported that seizure of VAs may be carried out under procedural powers corresponding to Article 19 of the Convention, particularly where VAs are regarded, at least in part, as computer data. In such cases, seizure may involve securing access credentials, seizing data carriers, or transferring assets to law enforcement-controlled wallets through the application of powers applicable to stored computer data.

In other jurisdictions, VAs are seized under general criminal procedure provisions governing seizure of property or objects, without explicitly linking seizure to computer data powers. In such cases, VAs are treated primarily as assets within the scope of ordinary seizure regimes.

In addition, several jurisdictions have introduced specific legislative provisions addressing seizure of digital assets as a distinct category. In some replies, these provisions are presented as implementation of procedural powers corresponding to Article 19 of the Convention. At the same time, the same provisions are described as forming part of broader domestic frameworks governing seizure, confiscation and recovery of criminal assets.

Notably:

- Australia introduced express provisions in the Crimes Act and the Proceeds of Crime Act permitting the seizure of “digital assets” under search warrants. These provisions allow digital assets to be seized by transferring them to a law enforcement-controlled wallet or by reconstructing a wallet using material found during a search. The framework also permits remote technical assistance and extended timeframes reflecting the complexity of digital forensic analysis.

- Canada established a special search warrant for digital assets enabling seizure of cryptocurrency as proceeds of crime. Warrants may be accompanied by assistance or management orders requiring VASPs to co-operate and transfer funds to a police-controlled wallet.

- France provides for a dedicated procedural regime (“saisie pénale spéciale”) applicable to digital assets under the CCP. This regime permits rapid seizure of

crypto-assets, including where there are plausible grounds to suspect imminent dissipation, and provides for judicial oversight.

- Serbia and Slovakia reported specific legislative provisions addressing seizure of digital assets within their criminal procedure frameworks.

Other jurisdictions apply existing criminal procedure or enforcement provisions to execute seizure without establishing a distinct digital asset seizure regime:

- In Liechtenstein, seizure is based on §96 of the Criminal Procedure Code (StPO). VAs may be secured under these general seizure provisions and transferred to secure wallets maintained by the National Police, including through the use of hardware devices.

- In the Netherlands, seizure of VAs is grounded in the general provisions of the DCCP and Penal Code. Once identified and traced, VAs may be seized by transferring them to a government-controlled wallet.

Taken together, the replies indicate three legislative techniques: reliance on powers applicable to stored computer data; application of general property seizure regimes; and adoption of tailored digital asset seizure provisions. In certain jurisdictions, these approaches overlap, reflecting the dual technical and economic dimensions of VAs.

3.2.4 Custodial management and realisation of seized virtual assets

Several jurisdictions described institutional arrangements for the management and administration of seized and forfeited VAs. The replies indicate that, once VAs are secured through seizure or freezing measures, dedicated authorities or asset management bodies are often responsible for preserving their value pending final confiscation or return.

For example:

- In Australia, restrained and forfeited assets (including cryptocurrency) are managed by the Australian Financial Security Authority (AFSA), acting as Official Trustee. AFSA is responsible for preserving the value of the assets until applications for confiscation orders have been considered. Once assets have been forfeited, AFSA is responsible for selling those assets and depositing the proceeds into the Confiscated Assets Account.

- In France, seized digital assets are transferred to the Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC), which is responsible for conservation, management and, where appropriate, sale of digital assets. AGRASC may conduct sales prior to final judgment if authorised by law, and proceeds may be used for victim compensation or credited to the state.

- Israel reported that seized VAs are transferred to police-controlled digital wallets and, due to their volatility, courts may authorise sale in order to preserve value.

- In Moldova, the Criminal Assets Recovery Agency is responsible for managing seized criminal assets, including VAs, and may contract specialised entities for evaluation and administration.

- In Slovakia, management of seized crypto-assets is entrusted to a dedicated authority under legislation governing administration of seized property to preserve or increase its value.

- In the United States, the U.S. Marshals Service serves as the primary custodian of seized and forfeited cryptocurrency for the Department of Justice's Asset Forfeiture Program. Seized digital assets may be liquidated, including for victim compensation or other authorised uses.

Several replies highlight that the volatility of VAs may require specific management decisions, including conversion into fiat currency or court-authorised sale prior to final confiscation.

At the same time, where confiscation does not ultimately occur, assets or their equivalent value may be returned to the lawful owner. Overall, the replies demonstrate that custodial management of VAs has been integrated into broader asset administration systems.

4 International co-operation

4.1 Use of the Budapest Convention as a legal basis for international co-operation concerning VASPs

Question 7 asked whether authorities use the Budapest Convention as a legal basis for requesting data from VASPs located in other Parties to the Convention.

While Question 5 examined the domestic use of procedural powers corresponding to Articles 16–21 of the Convention, this question shifts the focus to their corresponding international co-operation powers, namely whether the Convention serves as a legal basis for co-operation between Parties when seeking VASP-held data abroad.

The more specific tools available under Articles 29–34 of the Convention and under the Second Protocol are examined in Section 4.2.

4.1.1 Overview of the approaches

On the basis of the 44 replies received to this question:

- 25 jurisdictions[53] indicated that they use or can use the Convention on Cybercrime as a legal basis for requesting data from VASPs located in other Parties. Some of these jurisdictions report regular or frequent use [54], while others indicate that the Convention is used where necessary, particularly in cases where VASPs do not voluntarily comply[55].

- 13 jurisdictions[56] reported that they do not use the Convention tools in practice for requesting data from VASPs in other Parties. The reasons provided vary:

[53] Albania, Andorra, Armenia, Brazil, Finland, France, Georgia, Germany, Ghana, Hungary, Israel, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Morocco, Norway, Poland, Portugal, Romania, Serbia, Spain, Sri Lanka, Switzerland, and the United States.

[54] For example France.

[55] For example Hungary.

[56] Australia, Bulgaria, Canada, Costa Rica, Iceland, Ireland, Japan, Montenegro, Netherlands, Peru,

- reliance on voluntary co-operation channels or VASP portals[57];
- absence of practical experience to date[58];
- use of other international instruments[59];
- use of Convention tools in other contexts but not yet in co-operation with VASPs[60].

- The remaining jurisdictions did not clearly state their position.

The replies demonstrate that a majority of responding jurisdictions recognise that the Budapest Convention can serve as a legal basis for requesting data from VASPs located in other Parties. However, operational practice varies. In several jurisdictions, authorities report that voluntary co-operation channels or alternative frameworks are frequently relied upon in practice.

This suggests that while the Convention framework is widely acknowledged as legally applicable, its practical use in the specific context of VASP-related cross-border requests is not uniform across Parties.

4.1.2 Selected examples

The following examples illustrate the diversity of approaches reported:

- Australia indicated that while Article 29 is regularly used for requests to ISPs, it has not yet been used to request data from VASPs. Additionally, Australia has made two MLA request to another country in accordance with Articles 25 and 27 of the Budapest Convention in recent years on the basis that the crime type was within scope of Articles 2-11. However, the assistance sought did not involve VASPs and was otherwise beyond the scope of the types of assistance provided for under Articles 29-34 of the Budapest Convention.

- France reported that the Convention on Cybercrime constitutes the most frequently used legal basis for obtaining data from foreign VASPs (outside the EU) through international co-operation, and that the specialised cybercrime prosecution service uses the Convention tools daily.

- Germany reported that the Convention is not used to secure virtual assets for the most part. Rather, the portals or email-addresses provided by the VASPs are used instead.

- Ghana described that, where necessary, it uses the tools offered by the Convention on Cybercrime as a legal basis for requesting data from VASPs and other Parties.

- Hungary explained that in many cases the location of VASPs cannot be clearly established. Where VASPs co-operate voluntarily, direct requests are used. Where they do not comply, Hungary relies on the Convention as a basis for formal MLA.

Philippines, Sierra Leone, Slovakia, Tunisia.

[57] For example Bulgaria, Ireland (Ireland also not yet a Party to the BC), Montenegro, Costa Rica.

[58] For example Philippines, Sierra Leone.

[59] For example Peru.

[60] Australia, Iceland.

- Peru reported that the Convention tools have not been used as a legal basis for VASP-related requests, and that other instruments have been relied upon in relevant cases.

- Portugal reported that its Cybercrime Law transposes both the procedural and international co-operation provisions of the Convention, and that these provisions are used to request data from foreign VASPs located in Parties to the Convention, mirroring the use of domestic procedural tools for domestic VASPs.

- Romania reported that the Directorate for Investigating Organized Crime and Terrorism (DIICOT) has based requests for assistance to obtain data from VASPs.

- Serbia stated that it uses the procedural and legal tools provided by the Convention on Cybercrime to request data from VASPs in other Parties, leveraging mutual legal assistance and other co-operation mechanisms to support investigations involving digital assets.

- Switzerland stated that it uses Article 32 of the Convention as a legal basis for requesting data from VASPs in other Parties.

- Tunisia indicated that the Convention is not currently used as a formal legal basis for requesting data from foreign VASPs, and that international co-operation is conducted through other judicial and financial co-operation mechanisms.

- United States pointed out that to the extent that VASP data constitutes "evidence in electronic form of a criminal offense," the United States notes that it may be possible to use Articles 25 and 27 of the Budapest Convention to seek such evidence via mutual assistance from another Party. Under U.S. law, the tools of Articles 29 to 34 of the Convention on Cybercrime and the tools of Articles 7,8, and 9 of the Second Additional Protocol could only be used to the extent that a VASP is also operating as a service provider as defined in Article 1.

4.2 Use of Articles 29–34 of the Budapest Convention and the Second Additional Protocol in VASP-related cases

Question 8 asked jurisdictions to indicate which of the tools under Articles 29–34 of the Convention on Cybercrime and which tools of the Second Additional Protocol are used, or may be used, in relation to VASP-related requests, including the types of evidence that may be sought.

This question was included to examine more specifically how the Convention's international co-operation framework operates in practice in the VASP context. Following Section 4.1, which addressed whether the Convention serves as a legal basis for cross-border requests, this section analyses the application of individual co-operation tools provided under Articles 29–34 and the Second Additional Protocol.

In doing so, the replies also illustrate the distinction already noted in earlier sections of this study, namely between requests aimed at:

- VASP-held computer data (excluding the VAs themselves); and

- situations in which certain co-operation measures have been used in practice in a way that may affect the movement or control of VAs.

A number of jurisdictions provided detailed information on which Convention tools are used, or could be used, in relation to VASP-held data. The replies show considerable variation between the individual powers under Articles 29–34 of the Convention on Cybercrime. The following subsections therefore analyse each Article separately.

4.2.1 Expedited preservation of stored computer data (Art. 29 of the Budapest Convention)

4.2.1.1 Overview of approaches

On the basis of the replies, 26 jurisdictions[61] indicated that Article 29 is used or may be used in the context of co-operation with VASPs:

Among these, 15 jurisdictions explicitly described operational use of Article 29 in practice.

The replies indicate two principal patterns:

- Preservation of VASP-held data (subscriber/KYC, transaction history, traffic data), pending a formal MLA request or production order.

- Preservation with asset-protective effect, where preservation mechanisms were used in practice to prevent the movement of VAs themselves.

While most jurisdictions describe Article 29 primarily as a tool to preserve VASP-held stored computer data, a limited number of replies explicitly link preservation to preventing the movement of VAs in practice. For example:

- Germany indicated that in some cases a preservation request under Article 29 was used to prevent transactions from an incriminated wallet.

- Norway reported analogous use of Article 29, particularly where it was necessary to prevent current assets from being moved.

This distinction is relevant. Although Article 29 is generally used to preserve stored computer data, practice in some jurisdictions indicates that, depending on domestic implementation and operational context, preservation measures may also have a protective effect in relation to VAs pending further investigative steps.

4.2.1.2 Selected examples

- Albania reported using Article 29 (together with Article 30) to preserve stored computer data held by VASPs, including transaction records, wallet addresses and user activity logs.

[61] Albania, Andorra, Armenia, Brazil, Finland, France, Georgia, Germany, Ghana, Hungary, Israel, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Morocco, Norway, Peru, Poland, Portugal, Serbia, Spain, Sri Lanka, Switzerland, United States.

- France stated that the specialised cybercrime prosecution service uses Article 29 and the 24/7 Network to preserve data held by foreign digital asset service providers.
- Spain reported that Article 29 is used directly to request preservation of computer data from service providers, without requiring judicial authorisation under domestic law.
- Switzerland indicated that Swiss law enforcement regularly makes preservation requests abroad under Article 29 in VA-related matters.

4.2.2 Expedited disclosure of preserved traffic data (Art. 30 of the Budapest Convention)

4.2.2.1 Overview of approaches

Approximately 19 jurisdictions[62] indicated that Article 30 is used or may be used. Operational examples were more limited compared to Article 29.

Article 30 is generally described as complementary to Article 29 and used to obtain traffic data necessary to identify VASPs and communication paths.

4.2.2.2 Selected examples

- Israel reported using Articles 29 and 30 in conjunction to obtain client registration data, transaction history and financial reporting information.
- Morocco referred to Articles 29, 30 and 35 (24/7 Network) in the context of expedited preservation and co-operation.
- Moldova clarified that its authorities are entitled to communicate the preserved traffic data under Article 30 only on the basis of MLA.
- Sri Lanka confirmed use of Article 30 to expedite disclosure of preserved traffic data.

4.2.3 Mutual assistance regarding accessing of stored computer data (Art. 31 of the Budapest Convention)

4.2.3.1 Overview of approaches

Approximately 22 jurisdictions[63] indicated that Article 31 is used or may be used. Article 31 is frequently described as the principal mechanism for obtaining stored computer data held by foreign VASPs, particularly following preservation under Article 29.

In many replies, Article 31 is characterised as the formal MLA channel through which preserved data is subsequently accessed or disclosed.

[62] Albania, Andorra, Armenia, Brazil, Finland, France, Georgia, Ghana, Hungary, Israel, Mauritius, Moldova, Morocco, Peru, Poland, Portugal, Serbia, Sri Lanka, United States.

[63] Albania, Andorra, Armenia, Brazil, Finland, France, Georgia, Germany, Ghana, Hungary, Israel, Latvia, Mauritius, Moldova, Peru, Poland, Portugal, Romania, Serbia, Spain, Switzerland, United States.

Unlike Article 29 (where some jurisdictions linked preservation requests to the operational prevention of movement of VAs), reported practice under Article 31 primarily concerns access to stored computer data held by VASPs. One jurisdiction (Germany) referred to Articles 30 and 31 as being used as classical confiscation instruments/mechanisms .

4.2.3.2 Selected examples

- Portugal identified Article 31 as one of the most relevant measures for obtaining stored computer data from foreign VASPs.
- Romania reported that requests formulated by DIICOT in VASP investigations were based on Article 31.
- Serbia indicated that Article 31 enables obtaining subscriber data, transaction records, IP addresses and wallet information in cross-border investigations.
- Spain described Article 31 as the basis for transnational collection of stored data, typically channelled through MLA or EIO mechanisms.
- Switzerland confirmed regular use of Article 31 in requests for subscriber information, transaction reports and KYC data.

4.2.4 Trans-border access to stored computer data with consent or where publicly available (Art. 32 of the Budapest Convention)

4.2.4.1 Overview of approaches

Approximately 17 jurisdictions[64] indicated that Article 32 is used or may be used in the context of co-operation involving VASPs.

Article 32 differs structurally from Articles 29–31 in that it does not require a formal MLA request[65]. It allows:

- access to publicly available (open source) stored computer data, regardless of where the data is located geographically; and
- trans-border access to stored computer data with the lawful and voluntary consent of a person who has authority to disclose the data.

In the context of VAs, several replies suggest that Article 32 may be particularly relevant in relation to blockchain-based information, given that many blockchain transactions are publicly visible and technically accessible. In appropriate circumstances, this may allow access to publicly available stored computer data without the need for formal MLA procedures.

No jurisdiction explicitly reported using Article 32 as a legal basis for the seizure, transfer or confiscation of VAs as such.

---

[64] Albania, Andorra, Armenia, Brazil, Finland, Georgia, Germany, Ghana, Latvia, Liechtenstein, Mauritius, Moldova, Peru, Portugal, Serbia, Switzerland, United States.

[65] See the T-CY Guidance Note # 3 Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY on 2-3 December 2014.

4.2.4.2 Selected examples

- Albania stated that Article 32 may be useful where data is publicly available on blockchains.
-
- Finland pointed out that data from open sources may be useful in criminal investigation. With respect to Article 32.b, consent is not however often available and the suspect has no obligation to contribute to the solving an offence they have committed. The scope of use of the Article can be used on consent of other people involved, such as the victim of the crime.

- Georgia reported that its courts regularly invoke Article 32 in international production orders when a VASP is in a Party to the Budapest Convention. The reply suggests that Article 32 facilitates access in cases where voluntary co-operation or direct production orders are possible.

- Liechtenstein stated that its national police apply Article 32 (and where necessary, Article 29).

- Portugal indicated that Article 32 could be used, including in situations where consent is obtained to disclose all types of information.

- Switzerland confirmed that Swiss law enforcement authorities make regular requests abroad under Article 32, alongside Articles 29 and 31, in VASP-related investigations.

4.2.5 Mutual assistance regarding the real-time measures – real-time collection of traffic data and interception of content data (Art. 33 and 34 of the Budapest Convention)

4.2.5.1 Overview of approaches

Replies concerning mutual assistance for real-time measures, namely the real-time collection of traffic data (Art. 33) and interception of content data (Art. 34), show significantly lower levels of reference compared to previously discussed measures.

Approximately 13 jurisdictions[66] indicated that Articles 33 and 34 is used or may be used in the context of co-operation involving VASPs.

Compared to Articles 29 and 31, references to Articles 33 and 34 are less frequent. The replies suggest that Articles 33 and 34 play a more limited role in VASP-related investigations compared to preservation and stored-data access mechanisms.

Both provisions are oriented toward real-time monitoring of traffic or content data, whereas VASP-related co-operation appears to focus predominantly on stored transaction histories, subscriber information and account records. Accordingly, Articles 33 and 34 function as available but less frequently used tools in cross-border investigations involving VAs.

[66] Albania, Andorra, Armenia, Brazil, Finland, Ghana, Mauritius, Moldova, Peru, Portugal, Serbia, Switzerland, United States.

4.2.5.2 Selected examples

- Mauritius provided detailed information on its domestic legislative framework implementing both real-time collection of traffic data and interception of content data in accordance with Convention principles. Requests from foreign states may be executed by the central authority, subject to judicial authorisation.

- Moldova clarified that both real-time collection of traffic data and interception of content data are conducted based on MLA requests and require a court order.

- Serbia stated that it may use Convention tools, including those corresponding to Articles 29–34, including real-time collection of traffic data and interception measures where legally justified.

4.2.6 Second Additional Protocol to the Budapest Convention

4.2.6.1 Overview of approaches

Several jurisdictions referred to tools under the Second Protocol as relevant or potentially relevant in the context of co-operation involving VASPs. Based on the replies, approximately 11 jurisdictions[67] indicated that tools comparable to the Second Protocol or analogous mechanisms under domestic law, are used, available, or may be relied upon in VASP-related investigations.

It should also be noted that, for most jurisdictions, the Protocol has not yet been fully ratified or implemented domestically, and the references concern potential future use rather than established operational practice.

The replies nevertheless suggest that the Second Protocol is viewed as particularly relevant in the VASP context due to its emphasis on direct co-operation with service providers.

Overall, the Protocol is perceived as strengthening the co-operation framework applicable to VASPs in relation to disclosure of stored subscriber information and traffic data and co-operation in emergencies[68].

4.2.6.2 Selected examples

- Albania indicated that, once fully implemented, it intends to rely on Second Protocol tools to facilitate expedited requests for subscriber information and traffic data from foreign VASPs. It also referred to the potential use of joint investigation mechanisms in cases involving VAs across multiple jurisdictions.

- Germany identified Articles 6–9 of the Second Protocol as particularly relevant in practice, including for obtaining subscriber information, transaction histories, IP ownership data and related technical information, although full ratification is pending.

---

[67] Albania, Brazil, Finland, Germany, Lithuania, Peru, Portugal, Serbia, Spain, Tunisia, United States.

[68] One of the advantages of the emergency mutual assistance (Art. 10 of the Second Protocol) may be that it can be used to obtain additional forms of co-operation beyond computer data held by providers. See para 152 of the ER to the Second Protocol.

- Lithuania indicated that Second Protocol mechanisms may be used to obtain subscriber information linked to cryptocurrency wallets or accounts, transaction records (including wallet addresses, timestamps and transaction hashes), IP and device metadata, content (such as emails, messages and other communication), and account activity logs, highlighting usefulness of Articles 7, 9 and 10 of the Second Protocol in this respect.

- Peru and Portugal identified disclosure of subscriber information and expedited production of subscriber and traffic data as the most relevant Protocol mechanisms in VASP investigations and also noted usefulness of emergency procedures.

- Serbia referred specifically to the mechanism for disclosure of subscriber information under the Second Protocol as particularly relevant for identifying users of VASP accounts located in another Party.

- Spain indicated that the Second Protocol provisions concerning subscriber and traffic data may be applicable in appropriate cases.

- Tunisia stated that, although the Protocol has not yet been directly used in practice, it could facilitate disclosure of subscriber data, transaction information and account-related records from foreign VASPs in the future.

- United States clarified that tools under the Second Protocol may be used only to the extent that a VASP qualifies as a "service provider" within the meaning of the Protocol. The United States also highlighted that emergency mutual assistance mechanisms under the Protocol may be available to seek information from a VASP in another Party in an emergency.

4.2.7 What types of evidence relating to a virtual asset could be requested?

The replies indicate that, in the context of international co-operation under Articles 29–34 of the Convention and the Second Protocol, jurisdictions primarily request computer data held or accessible by VASPs, rather than the transfer or seizure of the VAs themselves. Across the reporting jurisdictions, the following categories of evidence were explicitly mentioned:

- Identification data, including name, date of birth, address, contact details, identification documents and customer due diligence (KYC/CDD) records;

- Account registration and account-related information, including account creation data, linked payment methods and verification records;

- Transaction records, including wallet addresses, transaction histories, transaction hashes, timestamps, transferred amounts and destination addresses;

- Other technical metadata, including IP addresses, login timestamps, device identifiers and geolocation data;

- Communications or content data, including communications between users and VASPs, where available.

A limited number of replies[69] also referred to preservation measures under Article 29 that in practice may prevent the movement of VAs pending further investigative action.

4.3 Use of the 24/7 Network under Article 35 of the Budapest Convention

Question 9 asked whether jurisdictions use the 24/7 Network established under Article 35 of the Convention on Cybercrime when requesting data from VASPs located in other Parties.

This question was included to examine the practical use of the Convention's expedited co-operation mechanism in the VASP context. The 24/7 Network is designed to facilitate immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, including the provision of technical advice, preservation requests and rapid coordination between competent authorities.

Given the transnational and time-sensitive nature of many VASP-related investigations, the 24/7 Network plays a significant role in supporting expedited preservation of VASP-held data and has the capability to facilitate swift execution of MLA requests.[70]

4.3.1 Overview of approaches

Out of 44 jurisdictions that provided replies:

- 21 jurisdictions[71] reported actively using the 24/7 Network for VASP-related requests.
- 6 jurisdictions[72] stated that use would be theoretically possible but has not yet occurred in practice.
- 12 jurisdictions[73] indicated that they do not use the 24/7 Network for requesting data from VASPs.
- Tunisia, having acceded to the Budapest Convention in 2024, indicated that operational procedures and coordination mechanisms are currently being finalised, with future use of the 24/7 Network in VASP-related co-operation envisaged.
- Remaining 4 jurisdictions did not provide specific information or reported no operational experience.

[69] Notably Germany and Norway.

[70] On the role of 24/7 Network contact points in facilitating of swift execution of MLA requests see for example T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 12th Plenary (2-3 December 2014), p. 131 and Cybercrime Convention Committee (T-CY), Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers, adopted by the T-CY at its 18th on 27-28 November 2017, p. 44.

[71] Albania, Andorra, Armenia, Australia, Brazil, Finland, France, Germany, Ghana, Hungary, Israel, Latvia, Moldova, Morocco, Peru, Poland, Serbia, Spain, Sri Lanka, Switzerland and Türkiye.

[72] Costa Rica, Mauritius, Montenegro, Netherlands, North Macedonia and Portugal.

[73] Bulgaria, Canada, Georgia, Iceland, Ireland, Japan, Liechtenstein, Lithuania, Norway, Sierra Leone, Slovakia and the United States.

Several replies indicated that their 24/7 contact point operates within specialised cybercrime or investigative structures. In the context of VASP-related investigations, which are frequently transnational and time-sensitive, such operational positioning appears particularly appropriate for facilitating rapid coordination and preservation of VASP-held data, as well as facilitating contacts with relevant VASPs in their territory.

Taken together, the replies suggest that while practice varies, the 24/7 Network is widely recognised as an available and adaptable channel in the VA context. Nearly half of responding jurisdictions already rely on it in VASP-related matters. Several others indicate readiness to expand its use. Given the speed and cross-border nature of VA investigations, the 24/7 Network appears particularly well suited to support timely international co-operation.

4.3.2 Selected examples

Among jurisdictions reporting active use, several provided illustrative examples demonstrating the practical relevance of the 24/7 Network in VASP investigations:

- Albania reported that its 24/7 contact point, located within the General State Police Directorate, actively handles requests in VASP-related matters.
- Andorra indicated that the 24/7 contact point can be used to expedite data preservation and requests involving VASPs.
- Armenia stated that its 24/7 contact points, operated by the Ministry of Internal Affairs and the Investigative Committee, directly co-operate with VASPs that voluntarily provide requested data.
- Australia reported that AFP Cybercrime Operations uses the 24/7 Network for all current international requests and would continue to do so in VASP-related cases.
- Brazil emphasised that investigations involving crypto assets are inherently complex and often cross multiple jurisdictions. Leveraging on the 24/7 Network is essential to ensuring efficient and timely access to such data in transnational cases.
- Finland pointed out that 24/7 contact points can be consulted to determine where a service provider is located and which authority is competent; verify whether the provider is known, reliable, and cooperative with local authorities; issue a data preservation order; establish whether the provider may be contacted directly with the consent of the state of location; or obtain that state's consent for taking cross-border measures.
- France reported systematic use of the 24/7 Network by specialised cybercrime investigation services, with its use progressively extending to other investigative units requiring access to foreign VASPs.
- Germany clarified that while public prosecutors do not use the 24/7 Network for requesting data directly from VASPs, certain police departments use it for preservation requests.
- Ghana, Israel, Latvia, Moldova, Poland, Sri Lanka and Türkiye confirmed use of the Network in the context of international co-operation, including VASP-related matters.

- Morocco specifically referred to use of the Network in relation to the expedited preservation of stored data.
- Peru provided a concrete example of operational coordination through the 24/7 Network with other Parties to the Convention to facilitate voluntary co-operation with several VASPs.
- Serbia described active utilisation of the Network to request urgent data from VASPs, including transaction histories, wallet information and user identification data.
- Spain indicated that the Network is used to facilitate access to foreign VASPs and to expedite police or preservation requests.
- Switzerland confirmed regular use of the 24/7 Network through its Central Operations Division in cross-border VASP investigations.

Overall, these replies show that in a significant number of jurisdictions the 24/7 Network functions as an operationally embedded channel for urgent cross-border coordination in VAs investigations.

4.3.3 Evolving practice

Six jurisdictions[74] indicated that although the 24/7 Network has not yet been used in VASP-related cases, it remains available and could be instrumental when necessary.

In several replies, authorities explained that direct voluntary co-operation with VASPs is often effective, reducing the immediate need to use the 24/7 Network. Nevertheless, the existence of an operational 24/7 channel provides an important option where voluntary co-operation is unavailable or where urgent preservation of data is required. Several replies also noted that the 24/7 Network is useful for contacting VASPs in a Party's territory.

Tunisia reported that following its recent accession to the Convention, operationalisation of the 24/7 contact point is underway. This signals clear readiness to incorporate the 24/7 Network into future VASP-related international co-operation.

4.4 Other international legal frameworks for evidence gathering and the search, seizure and confiscation of virtual assets

While Articles 29–34 of the Budapest Convention establish specific mechanisms for the preservation and access to electronic evidence, Chapter III of the Convention sets out a broader framework for international co-operation in investigations concerning criminal offences related to computer systems and data, or for the collection of electronic evidence[75].

[74] Costa Rica, Mauritius, Montenegro, Netherlands, North Macedonia and Portugal.

[75] Article 23 of the Budapest Convention entitled General principles relating to international co-operation reads as follows: "The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

Within this framework, the general mutual assistance provisions, and in particular Article 25, may serve as a legal basis for forms of mutual assistance not expressly addressed in the Convention's specific electronic evidence provisions, subject to the scope of the Convention and the domestic law of the requested Party.[76]

At the same time, VA investigations frequently involve measures such as freezing, seizure and confiscation that may also fall within the scope of other international legal instruments. Questions 10 and 11 therefore sought to identify additional international agreements and co-operation frameworks relied upon by jurisdictions in cross-border cases involving VASPs and VAs.

Question 10 asked which additional international instruments are relied upon for co-operation with VASPs located abroad, while Question 11 focused specifically on legal bases and procedures for the search, seizure and confiscation of VAs at international level.

These questions were included to identify the broader international co-operation landscape applicable to VA investigations beyond the framework of the Convention on Cybercrime.

While earlier sections examined co-operation under the Convention, including its procedural and international co-operation tools, many jurisdictions also rely on multilateral conventions, regional mutual recognition mechanisms, bilateral arrangements and operational co-operation channels when seeking evidence, freezing assets or pursuing confiscation in cross-border cases.

As several replies addressed Questions 10 and 11 jointly or referred to overlapping frameworks, the analysis below considers them together.

4.4.1 Overview of approaches

Across the replies, jurisdictions described a combination of co-operation mechanisms used both for obtaining data from VASPs outside their jurisdiction and for conducting freezing, seizure and confiscation measures, typically combining (i) treaty-based approaches (such as MLA), (ii) regional mechanisms or bilateral treaties, and (iii) operational co-operation channels (police-to-police and FIU-to-FIU).

In several replies, jurisdictions also emphasised that voluntary co-operation with VASPs remains operationally important, with formal frameworks used where voluntary co-operation is unavailable, insufficient, or where formal procedures are required to obtain admissible evidence.

Some jurisdictions did not provide a substantive response or noted limited experience to date.

[76] See for example para 264 of the ER to the Budapest Convention. "(…) Article 27 does not provide rules for other issues typically dealt with in domestic legislation governing international mutual assistance. For example, there are no provisions dealing with the form and contents of requests, taking of witness testimony in the requested or requesting Parties, the providing of official or business records, transfer of witnesses in custody, or assistance in confiscation matters. With respect to such issues, Article 25, paragraph 4 provides that absent a specific provision in this Chapter, the law of the requested Party shall govern specific modalities of providing that type of assistance."

4.4.2 Multilateral treaty frameworks and other standards

Council of Europe instruments were prominently cited among multilateral treaty bases. In particular:

- European Convention on Mutual Assistance in Criminal Matters (ETS No. 030)[77] was explicitly referenced by 5 jurisdictions[78]. Its additional protocols[79] may be also of relevance.

- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)[80] known also as Warsaw Convention was explicitly referenced by several jurisdictions[81] in connection with tracing, freezing, seizure and confiscation measures.

- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141)[82] was also mentioned in responses.

Beyond Council of Europe instruments, UN conventions featured regularly as legal bases applicable both to co-operation for obtaining evidence and to freezing, seizure and confiscation:

- United Nations Convention against Transnational Organized Crime[83] (UNTOC) was explicitly cited by multiple jurisdictions[84] as supporting international co-operation in tracing, freezing, seizure and confiscation of assets and related evidentiary measures.

---

[77] European Convention on Mutual Assistance in Criminal Matters (ETS No. 030).

[78] Albania, Andorra, France, Germany, Iceland

[79] See Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 099); Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182); Third Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 227).

[80] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198). It should be noted that this Convention is supplemented by an additional protocol (CETS No. 232) which introduces definitions of virtual assets and virtual asset service providers (VASPs) drawing on the FATF Recommendations and relevant EU acquis. The Protocol establishes mechanisms enabling the identification of persons holding virtual asset accounts and extends the powers of courts and competent authorities to access information on virtual assets transactions, and the identity of account holders and their beneficial owners. It also provides for the monitoring and suspension of virtual asset transactions and accounts in case of suspicion, including effective mechanisms for international co-operation. However, participation in the Warsaw Convention, as well as its future Protocol (to be opened for signature on 14 October 2026), is, at present, not as broad as participation in the Budapest Convention, while noting the complementary nature of the two frameworks.

[81] Albania, Germany, Moldova, Netherlands, Slovakia.

[82] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141).

[83] United Nations Convention against Transnational Organized Crime (2000).

[84] Albania, Andorra, Costa Rica, Finland, France, Netherlands, Norway, Peru, Serbia, Switzerland and Tunisia.

- United Nations Convention against Corruption[85] (UNCAC) was explicitly cited by several jurisdictions[86].

- The 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances [87]was additionally referenced[88] as part of the treaty framework for tracing seizure and confiscation measures.

United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (2024)[89] may also serve as a useful tool once it enters into force.

Standards-based and policy co-operation settings (e.g., FATF-related workstreams) were mentioned in some replies, particularly regarding VASP compliance expectations and practical co-operation.

4.4.3 Regional frameworks and bilateral agreements

Regional co-operation or regional mutual recognition tools were also frequently referenced.

In the EU context:

- EU co-operation instruments for evidence gathering (notably the European Investigation Order[90]) were explicitly cited by 10 jurisdictions[91].

- EU mutual recognition instruments relating to freezing and confiscation such as the Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders[92] or Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (relevant for intra-EU co-operation with Denmark and Ireland)[93] were explicitly cited by 4 jurisdictions[94]. These replies distinguish between EU cases, where mutual recognition mechanisms may be used, and non-EU cases, where classic MLA frameworks apply.

[85] United Nations Convention against Corruption (2003).

[86] Costa Rica, Finland, Norway, Peru, Serbia, Switzerland, Tunisia.

[87] United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988).

[88] For example by Peru.

[89] United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (2024).

[90] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[91] Bulgaria, France, Germany, Hungary, Lithuania, Poland, Portugal, Romania, Slovakia, Spain.

[92] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders.

[93] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence.

[94] France, Germany, Latvia, Netherlands.

- Convention on mutual assistance in criminal matters between EU Member States (2000)[95][96].

In the American region:

- Inter-American and Central American instruments, including the Inter-American Convention on Mutual Assistance in Criminal Matters[97], the Inter-American Convention against Corruption[98], and the Inter-American Convention against Terrorism[99], as legal bases relevant to co-operation in both evidentiary and asset-related contexts[100].

Several jurisdictions[101] also referred to the use of bilateral agreements.

Another jurisdiction[102] pointed out to use of reciprocity/domestic MLA acts where no treaty exists.

4.4.4 Operational co-operation channels

A substantial number of jurisdictions highlighted operational channels as important in practice, particularly for initial contact, coordination, and intelligence exchange:

- Police-to-police channels (such as Interpol/Europol and related channels) were explicitly referenced by 12 jurisdictions[103].

- FIU-to-FIU co-operation or Egmont-type channels were explicitly mentioned by 13 jurisdictions[104], frequently with the clarification that information exchanged via FIU channels may be intelligence-oriented rather than evidentiary in nature.

- Asset recovery practitioner networks (e.g., CARIN-type networks) were also referenced as supporting coordination in freezing/seizure/forfeiture contexts.[105]

4.4.5 Selected examples

- Australia described mutual legal assistance as the primary mechanism for requesting and providing assistance in VASP-held data as well as freezing, seizure and

[95] Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union.

[96] Explicitly referred to by Germany and Poland.

[97] Inter-American Convention on Mutual Assistance in Criminal Matters (1992).

[98] Inter-American Convention against Corruption (1996).

[99] Inter-American Convention against Terrorism (2002).

[100] Explicitly referred to by Costa Rica and Peru.

[101] Albania, Australia, Brazil, Costa Rica, Fiji, France, Germany, Japan, Latvia, Netherlands, Norway, Peru, Serbia, Slovakia, United States.

[102] Examples include Australia, Germany, Slovakia, Switzerland.

[103] Albania, Andorra, Canada, Iceland, Israel, Japan, Norway, Peru, Serbia, Switzerland, Tunisia, United States.

[104] Albania, Australia, Czechia, Fiji, Ireland, Japan, Liechtenstein, North Macedonia, Peru, Romania, Switzerland, Türkiye, United States.

[105] For example the United States.

confiscation of VA. Its reply outlined how domestic proceeds-of-crime legislation interacts with MLA procedures, including registration of foreign restraint or confiscation orders and requests for foreign authorities to act under their own laws.

- Canada highlighted Europol SIENA as a channel leveraged for information sharing and requests to Europol member states.

- France distinguished between EU and non-EU contexts for both VASP-held data and freezing/confiscation, using EU mutual recognition tools intra-EU and convention-based co-operation (including UNTOC) outside the EU. The reply also clarified that seized assets typically remain in the executing state and are managed according to its domestic legislation, with confiscation and liquidation procedures implemented thereafter.

- Germany described a structured set of EU co-operation instruments (including the EIO Directive and other EU co-operation measures) and, outside the EU, reliance on national mutual assistance law and the European MLA Convention (1959); it also noted that some operational co-operation with VASPs may occur on a voluntary basis without reliance on treaty instruments in specific instances.

- Latvia provided operational detail on custodial management, including transfer of seized VAs to a dedicated cold wallet operated by a state agency.

- Liechtenstein emphasised the role of financial regulatory co-operation (including administrative assistance and MoUs involving its Financial Market Authority), alongside engagement in Egmont and other regulatory co-operation settings.

- Netherlands cited bilateral arrangements with the United States, UN treaty bases (including UNTOC and the 1988 Vienna Convention), and participation in policy and standards-based co-operation settings including the FATF Virtual Asset Working Group.

- Norway pointed to a broad co-operation mix, including Europol/Eurojust, Interpol, and the potential relevance of UN conventions (explicitly UNTOC and UNCAC) and other thematic instruments (e.g., where applicable, the Lanzarote Convention).

- Switzerland indicated reliance on applicable MLA treaties and domestic MLA law, complemented by Interpol channels and FIU-to-FIU exchange through Egmont, especially for co-operation with a broader set of jurisdictions.

- Tunisia indicated reliance on the Convention on Cybercrime, bilateral and multilateral MLA frameworks, and FATF recommendations. It specified that VAs are seized through the competent foreign courts, held in secure wallets under judicial supervision, and may be confiscated or converted into fiat currency if necessary.

- United States described its central authority model for MLA (OIA) operating through bilateral and multilateral MLA instruments, supplemented by informal channels including law enforcement co-operation, asset recovery networks (e.g., CARIN), and Egmont.

4.5 Use of voluntary co-operation mechanisms in cross-border co-operation with VASPs?

Question 12 asked whether jurisdictions use voluntary co-operation mechanisms when requesting data from VASPs located outside their jurisdiction.

This question was included to examine the role of informal or voluntary co-operation in cross-border investigations involving VAs. In addition to formal international co-operation mechanisms under the Budapest Convention and other applicable frameworks, authorities may seek assistance through direct engagement with VASPs, including via dedicated portals or other non-compulsory mechanisms.

The relevance of this question lies in understanding how such voluntary co-operation operates in practice, including its interaction with formal MLA procedures and its potential impact on the speed, scope and evidentiary use of information obtained.

The section therefore examines the operational forms, practical benefits and limitations of voluntary co-operation in the VASP context, without prejudice to the continued relevance of formal international co-operation frameworks.

4.5.1 Overview of approaches

Out of 44 jurisdictions that provided replies:

- 39 jurisdictions[106] indicated that they use voluntary co-operation mechanisms when requesting data from VASPs outside their jurisdiction (in some cases with qualifications).

- 3 jurisdictions[107] indicated that they do not use voluntary co-operation mechanisms and prefer formal co-operation.

The replies demonstrate that voluntary co-operation is a frequently used model in cross-border VASP investigations.

The data further suggests that voluntary co-operation mechanisms have become an important component of cross-border VASP investigations. They are particularly valued for speed and flexibility, direct access to subscriber and transaction data, rapid freezing or flagging of VAs, avoidance of lengthy formal co-operation procedures.

At the same time, reliance on voluntary co-operation introduces variability. Responses depend on internal VASP policies, and several jurisdictions reported instances of delayed responses, non-response, or redirection to formal MLA channels. Moreover, information obtained through voluntary mechanisms may not always satisfy evidentiary requirements or may be used for intelligence purposes only.

[106] Albania, Andorra, Armenia, Australia, Brazil, Bulgaria, Costa Rica, Czechia, Fiji, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Ireland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Morocco, Netherlands, North Macedonia, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Sierra Leone, Spain, Switzerland, Tunisia and Türkiye.

[107] Canada, Slovakia and Sri Lanka.

Overall, voluntary co-operation frequently operates as a first-line mechanism in the VASP context, complemented where necessary by formal international co-operation channels.

4.5.2 Operational forms of voluntary co-operation

The replies indicate that voluntary co-operation in the VASP context primarily takes three operational forms:

- Direct voluntary requests for data held by VASPs: several jurisdictions described contacting VASPs directly, outside formal international co-operation procedures, to obtain computer data/evidentiary information. This typically occurs through dedicated law enforcement portals, private-sector platforms used by certain VASPs for structured law enforcement requests and, official email of VASP contact.[108]

- Voluntary freezing or securing of VAs: in addition to disclosure of data, several jurisdictions indicated that voluntary co-operation may extend to freezing or securing VAs.[109]

- FIU-based intelligence co-operation: a smaller group of jurisdictions[110] referred to voluntary co-operation through FIUs and the Egmont framework. In these cases, co-operation may take the form of intelligence-sharing via FIU channels. Such information may complement investigations but does not necessarily replace formal evidentiary mechanisms.

4.5.3 Limitations of voluntary co-operation

Despite its widespread use, several jurisdictions highlighted practical or legal limitations:

- Albania, which reported instances of non-response or that the use formal channels was requested.

- Andorra, which emphasised that co-operation depends on internal VASP policy.

- Canada, which generally requires domestic production orders even where voluntary disclosure may be possible.

- Netherlands, which avoids voluntary co-operation where possible for procedural reasons but may rely on it in urgent situations.

---

[108] This approach was explicitly referred to by Andorra, Australia, France, Ghana, Hungary, Israel, Peru, Philippines, Portugal, Romania, Serbia, Spain and Türkiye. For example, France reported routinely addressing direct requests to foreign VASPs and resorting to MLA only where voluntary co-operation fails. Spain and Romania referred to use of private-sector platforms, while Hungary and Türkiye described voluntary engagement as the primary or preferred mechanism for cross-border VASP data requests.

[109] This was explicitly described by France, Germany, Hungary, Israel, Norway, Peru and Serbia. Germany reported that certain VASPs voluntarily execute seizure or confiscation orders and may transfer assets directly to authorities' wallets. It also described notifying major VASPs of incriminated transaction IDs so that they may be flagged and rapidly frozen if received. France and Peru reported temporary freezing or seizure measures initiated through voluntary engagement before formalisation via MLA where necessary.

[110] Czechia, Romania, Türkiye and United States.

- Romania, where FIU-obtained information may be restricted to intelligence use.
- Slovakia, which reported unsuccessful attempts to obtain information via voluntary mechanisms.

These replies suggest that voluntary co-operation is operationally significant but not uniformly reliable and may require subsequent formalisation through MLA or other legal mechanisms.

4.6 Specific co-operation channels, portals or platforms provided by VASPs

Question 13 asked whether jurisdictions are aware of specific channels, portals or platforms provided by VASPs to facilitate co-operation with law enforcement authorities.

This question was included to identify whether structured communication mechanisms established by VASPs form part of the practical co-operation environment in VA investigations. Such channels may be used in the context of voluntary engagement but may also interact with formal co-operation frameworks.

The section therefore examines the types of channels identified and their practical relevance.

4.6.1 Overview of approaches

Out of 44 jurisdictions that provided replies:

- 38 jurisdictions[111] indicated that they are aware of specific channels, portals or platforms provided by VASPs to facilitate co-operation with competent authorities.
- The remaining jurisdictions either indicated that they are not aware of such platforms or did not provide detailed information identifying specific co-operation channels.

The replies demonstrate a high level of awareness of structured co-operation channels in the VASP context. In many jurisdictions, such channels appear to be integrated into operational practice and form part of the routine interaction between competent authorities and VASPs.

The responses further indicate that co-operation in the VA environment is increasingly facilitated through structured digital interfaces, including centralised request systems, VASP-operated portals, and designated compliance communication channels.

At the same time, awareness of such mechanisms does not necessarily imply uniform accessibility, responsiveness, or possibility to use the data obtained as evidence. The degree of reliance on these platforms varies across jurisdictions. Overall, the data suggests that platform-based engagement has become a significant feature of contemporary VASP-related investigations, although its operational use differs depending on domestic frameworks and institutional practice.

[111] Albania, Andorra, Armenia, Australia, Brazil, Bulgaria, Canada, Costa Rica, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Ireland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Montenegro, Morocco, Netherlands, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Slovakia, Spain, Switzerland, Türkiye and United States.

4.6.2 Types of co-operation channels identified

The replies indicate that jurisdictions are aware of a range of structured digital channels used by VASPs to facilitate co-operation with law enforcement authorities:

- Centralised digital platforms that enable submission of requests to multiple VASPs: a significant number of jurisdictions referred to structured online systems through which law enforcement authorities may submit requests via a unified interface covering several VASPs[112].

- VASP-operated portals and compliance channels: At least 25 jurisdictions[113] described awareness of VASP-operated portals, compliance teams, legal departments, or designated email addresses for official requests. These channels differ from centralised platforms in that they are operated by individual VASPs rather than providing a multi-exchange interface.

- Supporting investigative and coordination tools: a smaller number of jurisdictions[114] referred to tools that support investigations but are not themselves formal request portals. These include blockchain analytics software, internal databases cataloguing VASP contact points, and coordination platforms linked to Europol initiatives. These mechanisms assist in identifying transaction flows or relevant contact points but do not replace formal data-request procedures.

5 Legal challenges

5.1 Main legal challenges encountered in domestic and cross-border co-operation with VASPs

Question 14 asked jurisdictions to summarise the main legal challenges encountered when seeking to obtain information or evidence (a) from VASPs within their territory and (b) from VASPs located outside their jurisdiction, and to indicate how such challenges are addressed. The section therefore examines the reported obstacles in the application of procedural powers and international co-operation mechanisms, as well as measures taken to overcome them.

5.1.1 Challenges in obtaining information or evidence from VASPs within a Party's territory

The replies indicate that, at the domestic level, challenges are less frequently reported than in cross-border situations.

Some jurisdictions indicated few or no legal obstacles domestically[115].

---

[112] Approximately 20 jurisdictions (Australia, Brazil, Bulgaria, Canada, France, Georgia, Germany, Hungary, Ireland, Liechtenstein, Lithuania, Montenegro, Norway, Peru, Poland, Romania, Slovakia, Spain, Switzerland and United States) explicitly referred to such centralised platforms.

[113] Albania, Andorra, Australia, Brazil, Canada, France, Georgia, Germany, Ghana, Hungary, Iceland, Ireland, Israel, Japan, Latvia, Liechtenstein, Lithuania, Mauritius, Moldova, Montenegro, Morocco, Netherlands, Norway, Peru, Philippines, Poland, Portugal, Romania, Serbia, Spain, Switzerland and Türkiye.

[114] Albania, Germany and Hungary, among others.

[115] Armenia, Czechia and Bulgaria reported no legal challenges. Germany similarly reported no significant

Furthermore, based on some replies, domestic challenges may be limited because the domestic ecosystem is small or non-existent[116].

Where challenges were identified, they were related mostly to three main areas: regulatory gaps, co-operation and enforcement issues, and technical or operational limitations.

- Regulatory gaps and incomplete frameworks - several Parties linked domestic challenges to the absence of a comprehensive legal framework for VASPs or to gaps in coverage.[117]

- Non-co-operation and lack of enforcement mechanisms - several jurisdictions identified non-co-operation or limited enforcement capacity as key domestic challenges.[118]

- Technical and evidentiary challenges - some jurisdictions explicitly referred to technical constraints.[119]

5.1.2 Challenges in obtaining information or evidence) from VASPs located outside a Party's territory

The replies demonstrate that challenges are greater when VASPs are located outside national jurisdiction.

The most frequently cited obstacles relate to non-co-operation, jurisdictional ambiguity, and prolonged response times linked to formal mutual legal assistance procedures. Additional challenges concern legal diversity, limitations in freezing mechanisms, and insufficient identification or retention practices.

---

domestic legal challenges, noting that recent legal amendments have standardised the classification of cryptocurrencies and the obligations of VASPs, thereby addressing earlier difficulties.

[116] Mauritius reported that there are currently no VASPs in the country; Latvia noted there is no active local VASP; Hungary indicated that there are no large cryptocurrency providers and no significant organisational presence in practice.

[117] Albania referred to an incomplete framework that does not cover all categories of VASPs and highlighted uncertainties around supervisory responsibilities. North Macedonia highlighted the need for amendments to procedural and substantive legislation to ensure proper recognition, valuation and confiscation of crypto-assets. Sierra Leone described the sector as previously unregulated and only recently addressed under AML legislation.

[118] Ghana referred to insistence on court orders even for emergency requests and non-compliance by certain exchanges. Ireland described difficulties with VASPs retaining limited KYC documentation and the increasing use of intermediary services that obscure transactional information. Israel noted challenges involving unlicensed operators and licensed entities operating beyond their authorisation. Türkiye mentioned variable or late responses to information requests.

[119] Canada noted uncertainty around courtroom use of blockchain-based evidence and limited precedents regarding the admission of digital asset evidence. Romania stressed that enforcement becomes practically difficult where assets are in self-custodial wallets without access to private keys and noted the absence of a centralised database for VAs. Türkiye referred to variable response times or late responses to information requests.

- Non-co-operative VASPs and non-co-operative jurisdictions - a frequent reply is the lack of response, especially from VASPs located in offshore or otherwise difficult jurisdictions.[120]

- Unclear jurisdiction and corporate structure – several responses highlighted uncertainty regarding the location of VASPs or their legal entities.[121]

- Prolonged response times and MLA delays - multiple responses underlined the time-consuming nature of formal mutual legal assistance.[122]

- Need for rapid action and lack of fund-freezing mechanisms - several replies underscore that speed is often decisive.[123]

- Legal diversity and differing co-operation models - some jurisdictions pointed to differences in legal frameworks and co-operation models.[124]

- Limited KYC and insufficient retention policies[125]

Overall, the replies indicate that cross-border investigations face structural challenges linked to fragmentation of regulatory frameworks, jurisdictional ambiguity, non-co-operation and delays in obtaining assistance.

[120] Georgia highlighted lack of enforcement where non-co-operative VASPs are based in jurisdictions that are themselves non-co-operative via MLA. In one such case it was also impossible to determine the relevant jurisdiction. Portugal referred to VASPs without a clear connection to a particular country, offshore locations and limitations of voluntary co-operation. Canada noted that some VASPs do not reply or respond inconsistently and that some are in jurisdictions with difficult co-operation or without bilateral MLATs. Romania stated that certain platforms do not respond even to requests sent via formal international co-operation channels. Several other Parties referenced offshore jurisdictions and practical non-responsiveness.

[121] France described difficulties in identifying the competent legal entity and noted that some providers maintain ambiguity about the location of their headquarters. Germany similarly reported that it is often unclear where a VASP's official headquarters are located. Japan indicated that in some cases the location of the VASP and the relevant treaty partner cannot be determined at all.

[122] Australia described MLA as often lengthy, creating risks of evidence loss or asset dissipation. Brazil and Poland noted that formal procedures may be slower and less effective than direct approaches, yet voluntary co-operation is not always forthcoming. Romania referred to delays of up to one year in receiving responses through letters of request or EIOs.

[123] France indicated that the temporary freezing of assets may rely on voluntary co-operation, and stressed that, unless the assets qualify as computer data, there appears to be no clear basis for such action under the Budapest Convention. Nevertheless, this temporary freezing remains operationally significant when responses to MLA requests are delayed.

[124] Switzerland distinguished between jurisdictions permitting direct co-operation and those requiring MLA, emphasising that co-operation is more efficient where direct contact is possible thanks to the Budapest Convention framework (Switzerland relies on Article 32 of the Budapest Convention).

[125] Ireland, Japan and Germany noted limited KYC practices or insufficient retention policies. Germany also referred to concealment methods such as coin mixing and transaction splitting, which complicate tracing.

5.1.3 Overcoming these challenges

The replies describe a range of measures adopted to address both domestic and cross-border challenges. These measures include legislative reforms, use of co-operation channels under the Budapest Convention framework, and operational or technical strategies.

- Strengthening domestic legal frameworks - several replies pointed to legislative reforms or ongoing regulatory development as a key mitigation measure.[126]

- Use of international co-operation channels and the 24/7 Network - several replies highlighted the use of co-operation mechanisms under the Budapest Convention, including the 24/7 Network, as it has played an important role securing responses in a more efficient manner.

- Capacity building and technical tools - several replies stressed the importance of specialised expertise and tools. Peru referred to technical training and blockchain analysis software. Other responses suggested that improved technical capacity enhances tracing and evidence gathering.

- Regulatory leverage and sanctions - some jurisdictions described approaches to incentivise or compel co-operation.[127]

- Combining formal processes with informal engagement and public–private co-operation - several responses described the practical importance of outreach and informal co-operation with VASPs.[128]

Taken together, the replies indicate that effective access to information from VASPs depends not only on formal domestic procedural powers but also on operational readiness and structured co-operation mechanisms.

In cross-border contexts in particular, Parties frequently rely on the co-operation framework of the Budapest Convention, including the 24/7 Network, to facilitate faster communication. At the same time, several responses point to the continued relevance of international co-operation provisions and to the potential role of enhanced co-operation tools, such as those provided for under the Second Protocol to the Budapest Convention.

While domestic challenges are often described as manageable, cross-border access to evidence remains more complex and closely linked to the effectiveness of international coordination mechanisms.

---

[126] Germany linked improved domestic co-operation to legal amendments standardising the legal classification of cryptocurrencies and clarifying VASP obligations. Peru indicated the need to regulate licensing and registration of VASPs and referred to implementing legislative measures connected with enhanced international co-operation tools.

[127] Peru referred to the possibility of administrative or criminal sanctions and to introducing retention obligations. The Philippines mentioned potential penalties for unresponsive licensed entities.

[128] The Philippines emphasised strengthening informal co-operation mechanisms, including identifying appropriate points of service for production orders. United States described training, education and public–private partnerships, including outreach to VASPs on transaction monitoring and screening tools. Norway referred to increased competence and internal information sharing within police and prosecution services as contributing to more effective case handling.

5.2 Timeframes for compliance by VASPs with requests or orders

Question 15 asked jurisdictions to provide an indication of the approximate time required for VASPs to comply with requests or orders. This question was included to assess the timelines associated with obtaining data in the VASP context, considering different legal channels, including domestic powers, voluntary co-operation and international co-operation mechanisms. The section summarises reported response times and the factors influencing them.

5.2.1 Overview of approaches

The replies indicate that timeframes vary considerably across jurisdictions. Most jurisdictions emphasised that no single average timeframe can be identified, as response times depend on whether the request is domestic or cross-border, the cooperativeness of the VASP, the legal channel used (e.g. 24/7 Network, formal MLA, informal contact, dedicated portals), the scope of the request, and the urgency of the measure.

Overall, the replies suggest four broad patterns:

- Very rapid response time (hours to 1–2 days) primarily in urgent domestic contexts or where established co-operation channels exist. This is particularly the case where VASPs are licensed and subject to supervision, or where emergency freezing or preservation measures are involved.[129]

- Short-term response time (several days to two weeks) for routine domestic requests particularly for subscriber information, including KYC data or transaction histories[130].

- Medium-term response time (several weeks to a few months) in more complex cases or in cross-border situations where co-operation takes place through informal channels or the 24/7 Network but requires additional legal or technical review[131].

- Long-term response time (many months to years) where formal MLA is used or co-operation is limited[132].

---

[129] For example, Canada and Iceland referred to responses within 24 hours; France indicated that responses may in some cases be received within minutes; Germany and Norway reported responses within hours where the VASP is co-operative; and Peru indicated that administrative freezing measures issued by its Financial Intelligence Unit (Administrative Freezing of Funds – CAF) must be complied with within 24 hours.

[130] Philippines indicated 1–7 days; Ghana and Hungary reported one to two weeks; Serbia indicated three to seven days for simple requests; Switzerland referred to ten business days (with possible extension); and Liechtenstein and Lithuania reported approximately two to four weeks. In some jurisdictions, compliance is linked to statutory or regulatory deadlines. For example, Australia reported that notices issued under AML/CTF legislation by AUSTRAC generally provide 2–4 weeks for compliance, and some jurisdictions indicated fixed time limits for domestic production orders (e.g. 10 to 14 business days).

[131] Australia referred to one to three months in some cases; France to several weeks or months depending on scope and workload; Georgia reported cases exceeding one month (up to three months); and Tunisia referred to weeks to several months for foreign-based VASPs

[132] Germany and the United States reported that formal MLA may take several months or even years;

The factors most frequently cited as influencing timelines include:

- whether the VASP is licensed and regulated domestically;[133]
- the clarity and scope of the request;[134]
- the existence of a dedicated channel or portal;[135]
- the urgency of the measure;[136]
- the complexity of data extraction and internal review processes;[137]
- reliance on MLA mechanisms.[138]

Taken together, the replies illustrate that while domestic access to VASP-held data is often comparatively rapid, cross-border access remains significantly more time-consuming and less predictable.

6 Findings and recommendations

6.1 Findings

6.1.1 Legal classification of virtual assets and virtual asset service providers

The replies reflect differing domestic approaches to the legal classification of virtual assets (VAs) and virtual asset service providers (VASPs).

VAs are treated in domestic law variously as property/assets, as computer data, or as both. Their treatment as property or assets does not preclude their qualification as "computer data" for the purposes of the Convention, and vice versa. This dual character has practical implications for the types of measures applied in investigations. They may affect whether measures are directed primarily at VASP-held computer data or may also extend to targeting VAs themselves.

Japan indicated an average of approximately 160 days for MLA requests to foreign-based VASPs; Montenegro referred to MLA lasting one year or more; and Mauritius estimated that compliance may exceed one year in certain contexts. Several jurisdictions also noted that certain VASPs do not respond to voluntary or informal requests at all.

[133] Israel and Australia noted that licensed domestic VASPs generally comply more predictably and rapidly, while Latvia and Portugal pointed to variability depending on the provider's co-operation policy.

[134] France and Albania highlighted that the number of wallet addresses, transaction complexity and need for follow-up exchanges affect response times; Serbia similarly referred to the volume of data requested.

[135] 24/7 Network under the Budapest Convention may facilitate co-operation. Jurisdictions indicated also use of various platforms that are used for co-operation with VASPs.

[136] Peru, Canada, and Iceland referred to particularly rapid responses in urgent cases, especially where freezing or preservation measures are involved.

[137] Albania, France, and Australia emphasised technical and organisational factors affecting the response time.

[138] Germany, Japan, Montenegro, and the United States explicitly linked extended timeframes to formal MLA procedures.

Approaches to the qualification of VASPs also vary. Some jurisdictions explicitly consider VASPs to fall within the notion of "service provider" as defined by Article 1.c of the Convention. Others exclude them from this definition. Another group assesses the issue on a functional, case-by-case basis. A significant number of replies have not explicitly addressed the question.

At the same time, the applicability of procedural and co-operation provisions under the Convention does not apply exclusively to "service provider" but to natural and/or legal persons more broadly. Several measures, including production orders directed to "any person" and search and seizure powers relating to stored computer data, may apply irrespective of whether a VASP is considered to fall within Article 1.c. The qualification/disqualification of VASPS as "service providers" according to Article 1.c primarily affects the use of specific tools expressly addressed to service providers under the Convention and its Second Protocol.

The replies further indicate that VASPs widely are subject to AML/CFT frameworks implementing FATF Recommendations. These regulatory regimes and the Budapest Convention operate in distinct but complementary spheres. While AML/CFT frameworks impose preventive obligations on VASPs to collect and retain customer and transaction-related information, the Budapest Convention provides procedural and co-operation tools for criminal investigations and proceedings. The applicability of one framework does not preclude the application of the other. In practice, implementation of AML/CFT obligations may enhance the availability of data that can be sought through Convention-based measures.

6.1.2 Use of domestic procedural powers corresponding to the Budapest Convention

The replies indicate broad reliance on domestic procedural powers corresponding to Articles 16–21 of the Convention in investigations involving VASPs and VAs.

A clear majority of responding jurisdictions report that non-real-time measures, in particular preservation (Articles 16–17), production orders (Article 18), and search and seizure of stored computer data (Article 19), can be applied to preserve or obtain data held by VASPs. These measures are consistently used in practice.

The types of data typically sought include subscriber and customer due diligence (KYC/CDD) information, account identifiers, transaction histories, wallet-related records, IP logs and other technical metadata.

In a smaller number of Parties, powers corresponding to expedited preservation and search and seizure of stored computer data are also reported to be used in ways that secure control over VAs themselves, including through operational steps such as transfer to law enforcement-controlled wallets, depending on domestic law.

The use of real-time measures (Articles 20–21) in VA/VASP-related cases is possible in several jurisdictions; however, their application in these instances appears to be less frequent than that of measures concerning stored data.

Overall, the replies demonstrate that Budapest Convention-type procedural powers provide an established and operationally relevant framework for obtaining electronic evidence in VA/VASP-related investigations.

6.1.3 Domestic seizure, freezing and asset recovery frameworks

In addition to procedural powers for obtaining electronic evidence, Parties report relying extensively on broader domestic seizure, freezing and confiscation regimes when dealing with VAs.

The replies reflect three principal legislative techniques when it comes to the seizure of VAs:

- reliance on powers applicable to stored computer data (in some cases framed as implementation of Article 19-type measures);
- application of general property seizure regimes; and
- adoption of specific legislative provisions addressing seizure of digital assets as a distinct category.

In many Parties, confiscation and asset recovery of VAs are addressed within existing proceeds-of-crime frameworks, while some jurisdictions have introduced tailored digital asset seizure provisions. These approaches often overlap, reflecting technical and economic characteristics of VAs.

Replies further indicate that measures aimed at securing access credentials or stored computer data may operate in parallel with broader freezing and confiscation mechanisms addressing the economic dimension of the assets.

6.1.4 International co-operation under the Budapest Convention and its Second Protocol

The replies indicate that the Budapest Convention is widely recognised as a relevant legal basis for international co-operation in VASP-related cases.

Many jurisdictions reported that they use or can use the Convention as a legal basis for requesting data from VASPs located in other Parties. Operational practice varies: some Parties report regular use of Convention tools, while others rely frequently on voluntary co-operation or alternative frameworks, turning to formal Convention-based co-operation where necessary.

In practice, co-operation under Articles 29–31 is most prominent, reflecting the importance of expedited preservation and access to stored VASP-held computer data in cross-border investigations. Requests primarily concern subscriber and KYC data, account and transaction records, and related technical metadata.

While preservation requests under Article 29 are generally directed at VASP-held data, a limited number of replies indicate that preservation mechanisms may in practice also have an asset-protective effect, for example by helping prevent loss of VAs pending further measures, depending on domestic law and operational practice.

Article 32 of the Convention is highlighted by several jurisdictions as particularly relevant in VA investigations. Given that many blockchain transactions are publicly visible, the possibility of accessing publicly available stored computer data without formal MLA (according to Article 32.a) may facilitate investigative steps in cross-border contexts. Article 32.b may be relevant where lawful and voluntary consent is obtained from a person authorised to disclose stored data.

Although the Second Protocol to the Budapest Convention has not yet been ratified and implemented in many jurisdictions, replies suggest that it is regarded in some countries as particularly relevant in the VASP context, to the extent that VASP meets the definition of a

service provider in the context of direct co-operation with service providers (Article 7) and expedited disclosure of subscriber and traffic data (Article 8). The Second Additional Protocol is viewed as strengthening and modernising the co-operation framework applicable to cross-border VA investigations.

More broadly, while Articles 29–34 of the Convention establish specific mechanisms for the preservation and access to electronic evidence, Chapter III of the Convention provides a general framework for international co-operation in investigations concerning offences related to computer systems and data, or for the collection of electronic evidence. Within this framework, the general mutual assistance provisions (and in particular Article 25) may serve as a legal basis for forms of MLA not expressly addressed in the Convention's specific electronic evidence provisions, subject to the scope of the Convention and the domestic law of the requested Party.

This broader framework allows the Budapest Convention to operate alongside domestic procedures and other applicable instruments, including where assistance may relate, in appropriate cases and in accordance with domestic law, to measures such as freezing or securing assets. However, in light of its extensive participation, the Budapest Convention may be, in some cases, the only relevant treaty basis for co-operation where Parties do not share other bilateral or regional instruments.

6.1.5 Use of other international instruments for evidence gathering and the search, seizure and confiscation of virtual assets

The replies indicate that VA-related investigations frequently involve parallel reliance on other international legal frameworks, particularly where freezing, seizure and confiscation measures are concerned.

Council of Europe instruments, notably the European Convention on Mutual Assistance in Criminal Matters (ETS No. 30) and the Warsaw Convention (CETS No. 198), were cited by several Parties in connection with tracing, freezing, seizure and confiscation measures.

United Nations conventions and, in the context of regional instruments, mutual recognition tools for evidence gathering, conventions on mutual co-operation in criminal matters or asset measures were also referenced as part of the broader co-operation landscape. Jurisdictions also rely on the use of bilateral instruments.

The replies suggest that, in practice, co-operation in VA cases often combines electronic evidence tools under the Budapest Convention with complementary treaty frameworks addressing asset recovery.

6.1.6 Role of the 24/7 Network

The 24/7 Network under Article 35 is widely recognised as an operationally relevant channel in the VASP context.

Many jurisdictions reported actively using the Network for VASP-related requests, particularly in time-sensitive cross-border cases. The Network is used for rapid coordination, technical advice and preservation requests, and to support MLA processes where needed.

Replies also indicate that the 24/7 Network can facilitate contact with relevant VASPs located in the requested Party's territory and may support voluntary co-operation efforts in practice.

Given the speed and cross-border nature of many VA investigations, the 24/7 Network appears particularly well suited to support timely and practical international coordination.

6.1.7 Voluntary co-operation with VASPs

Voluntary co-operation mechanisms are widely used in cross-border VASP-related investigations.

Many jurisdictions reported using voluntary co-operation when requesting data from foreign VASPs. Such co-operation typically takes the form of direct requests via dedicated law enforcement portals, compliance channels and/or designated contact points. In some cases, voluntary co-operation may also extend to temporary freezing or flagging of VAs.

Voluntary co-operation is valued for its speed and flexibility and often functions as a first-line mechanism. At the same time, replies highlight variability in responsiveness and the need, in some cases, to formalise co-operation through MLA to ensure evidentiary admissibility or compliance with domestic legal requirements.

6.1.8 Legal challenges

The replies identify recurring challenges in VA/VASP-related investigations, including:

- differing domestic classifications and interpretations of relevant data categories;
- difficulties in identifying the location of VASPs or competent jurisdictions;
- technical and operational challenges, including issues related to decentralised environments and custody of digital assets; and
- challenges in ensuring timely and admissible cross-border co-operation.

At the same time, the replies demonstrate that Parties are making use of existing Budapest Convention tools and domestic frameworks to address these challenges in practice.

It is also anticipated that the future Additional Protocol to the Warsaw Convention could help mitigate several of the identified legal challenges, particularly those concerning the identification of VASPs' locations, the determination of competent jurisdictions, and facilitation of timely international co-operation.

6.2 Recommendations

Based on the mapping of current practices, the following actions may be considered at the level of the Council of Europe and the Cybercrime Convention Committee (T-CY):

Rec 1 The T-CY should continue its discussion on issues related to VAs and VASPs, with the aim of fostering a shared understanding and exploring possible measures in support of the effective use of the Budapest Convention and its Second Protocol in this context, and invite the T-CY Bureau to actively support this work, including by preparing and presenting possible elements and options for further work on this topic.

Rec 2 Parties are encouraged to make systematic and proactive use of Article 35 by engaging the 24/7 contact points for rapid co-operation, technical advice and urgent measures in VA/VASP-related investigations. The 24/7 Network may support the swift execution of MLA under the Convention, as well as expedited preservation, access to stored computer data, and other forms of mutual assistance, including in relation to seizure,

freezing or confiscation measures as permitted by the domestic law of the requested Party. Parties may also consider strengthening coordination between 24/7 contact points and other competent authorities involved in cybercrime and financial investigations, as appropriate within domestic frameworks.

Rec 3 Given the complementarity between the Budapest Convention and other applicable international instruments, Parties to the Budapest Convention and the Secretariat may consider promoting practical synergies in VA and VASP-related cases, including:

- raising awareness of how electronic evidence tools under the Budapest Convention can be used in conjunction with asset-related measures under other relevant instruments, such as the Warsaw Convention (CETS No. 198);
- enhancing coordination among competent authorities responsible for cybercrime investigations, international co-operation and asset recovery and management in order to ensure consistent and timely use of available tools;
- reflecting these complementarities in capacity-building activities and policy guidance.

Rec 4 Parties to the Budapest Convention should continue and further develop targeted training for investigators, prosecutors and judges on applying Convention procedural and co-operation provisions in VA/VASP contexts. The Council of Europe through its C-PROC should continue to support such capacity building activities. T-CY members may also wish to share the present study among relevant institutions within their countries.

Rec 5 Parties to the Budapest Convention may consider promoting structured engagement with VASPs to enhance clarity, predictability and efficiency of co-operation, including through:

- use of secure portals and designated compliance channels;
- development and promotion of standardised request formats, where appropriate;
- ensuring that voluntary co-operation mechanisms operate in complementarity with co-operation under the Convention and its Protocol.

7 References/sources

7.1 Relevant international instruments

7.1.1 Council of Europe legally binding instruments

European Convention on Mutual Assistance in Criminal Matters (ETS No. 030).

Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 099).

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141).

Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182).

Convention on Cybercrime (ETS No. 185).

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198).

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

Third Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS No. 227).

Additional Protocol to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (to be opened for signature on 14 October 2026).

7.1.2 United Nations legal instruments

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988).

United Nations Convention against Transnational Organized Crime (2000).

United Nations Convention against Corruption (2003).

United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (2024).

7.1.3 EU legal instruments

Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union.

Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European

Union of orders freezing property or evidence.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders.

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

7.1.4 Legal instruments adopted in the framework of other international regional organizations (OAS)

Inter-American Convention on Mutual Assistance in Criminal Matters (1992).

Inter-American Convention against Corruption (1996).

Inter-American Convention against Terrorism (2002).

7.1.5 Financial Action Task Force Standards

FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 2012-2025.

7.2 Relevant documents

7.2.1 T-CY reports and documents

T-CY Guidance Note # 3 Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY on 2-3 December 2014.

T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 12th Plenary (2-3 December 2014).

Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers, adopted by the T-CY at its 18th on 27-28 November 2017.

T-CY Guidance Note #12 Aspects of ransomware covered by the Budapest Convention, adopted by the 27th Plenary of the T-CY on 29-30 November 2022).

T-CY Assessment Report: Assessing Article 19 Budapest Convention on the search and seizure of stored computer data, adopted by the 31st T-CY Plenary of the T-CY on 12 December 2024.

T-CY Workplan for the period January 2026 – December 2027, adopted by the 33rd T-CY Plenary on 13-14 November 2025.

7.2.2 Council of Europe reports

MONEYVAL, Money Laundering and Terrorist Financing Risks in the World of Virtual Assets. Typologies report, 2023.

MONEYVAL, Practice of Using Virtual Assets, Virtual Asset Service Providers in the Laundering of Criminal Property, Financing of Terrorism, and the Evasion of Sanctions. Typologies report, 2025.

Economic Crime and Cooperation Division– Report on Crypto-assets and decentralised finance: Impact on money laundering and terrorist financing investigations led by Financial Intelligence Units, 2025.

7.2.3 FATF reports

FATF, Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity: VACG ROADMAP: JURISDICTIONS WITH MATERIALLY IMPORTANT VIRTUAL ASSET ACTIVITY (fatf-gafi.org) , 2024.

FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, 2025.