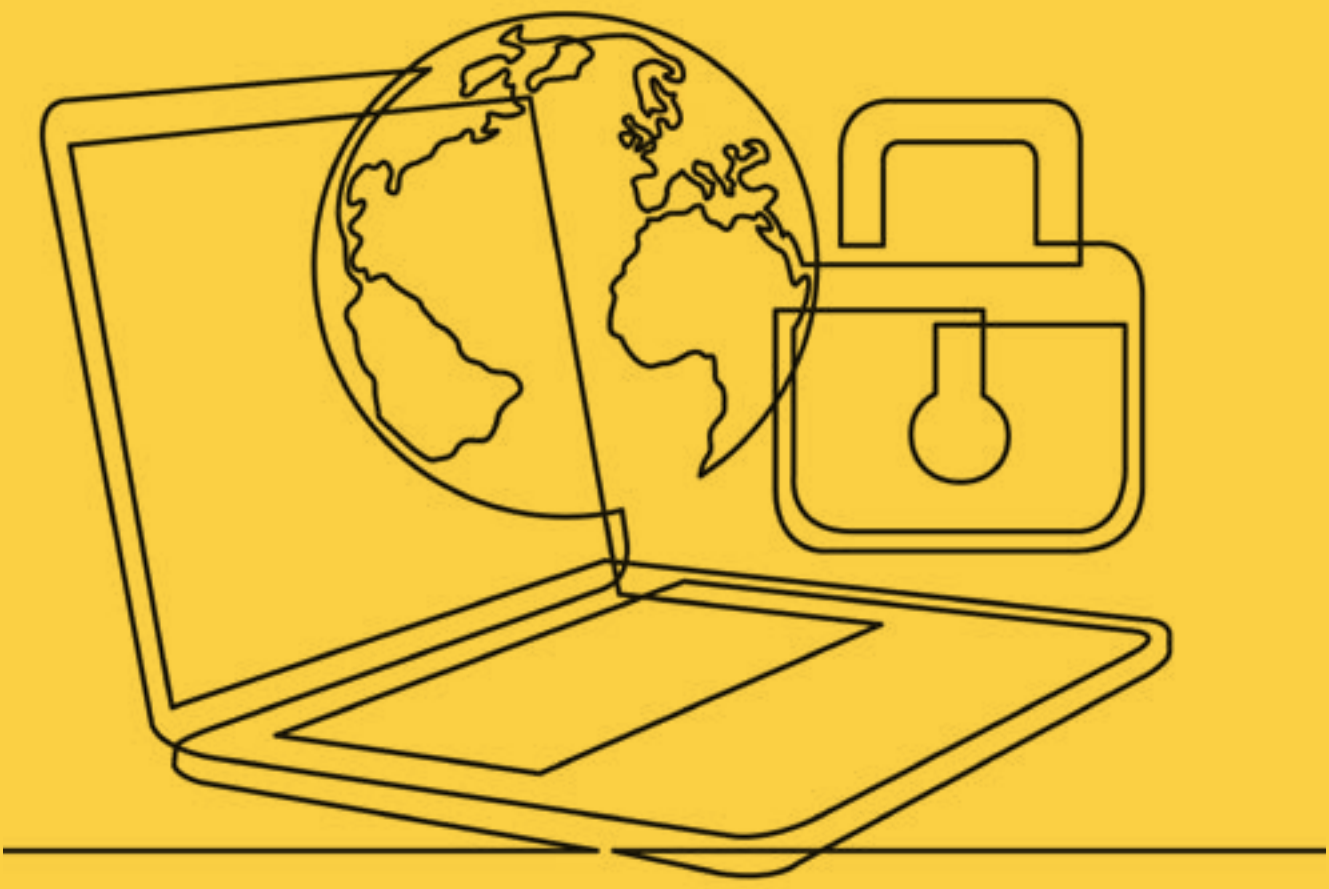
ELI
EUROPEAN
LAW
INSTITUTE

ELI Principles and Guidance for Enforcement Against Digital Assets

European Law Institute



The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct, and facilitate research, make recommendations, and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment, it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines, and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

European Law Institute
Schottenring 16/175
1010 Vienna
Austria
Tel: + 43 1 4277 22101
E-mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

ISBN: 978-3-9505495-5-3

P-2019-18b

Approved by the ELI Council on 2 March 2025 and by the ELI Membership on 8 May 2025.
Published on 12 June 2025.

This publication was co-funded by the European Union's Justice Programme. Acknowledgement is also due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011. Views and opinions expressed are those of ELI 's only and do not necessarily reflect those of the European Union, the University of Vienna or others. Neither the European Union nor others can be held responsible for them.

This project is co-funded by
the European Union

Table of Contents

Acknowledgements

Project Team
Project Reporters
Teresa Rodríguez de las Heras Ballell (as of September 2022; Professor, Spain)
Jos Uitdehaag (First Vice-President of the International Union of Judicial Officers (UIHJ), The Netherlands)
Sjef van Erp (until September 2022; Emeritus Professor, The Netherlands)

Other Members of the Project Team
Phoebus Athanassiou (Principal Legal Counsel, Germany)
Gabriele Della Morte (Professor, Italy)
Wian Erlank (Professor, South Africa)
Sabine Heijning (Legal Advisor, The Netherlands)
Teemu Juutilainen (Professor, Finland)
Paul Matthews (Professor, United Kingdom)
Thomas Meyer (Program Manager, Germany)
Christopher Mondschein (Researcher, The Netherlands)
Chris Odinet (Professor, United States of America)
Denis Philippe (Lawyer, Belgium)
Radim Polčák (Professor; Czech Republic)
Albert Ruda (Professor, Spain)
Cayetana Santaolalla Montoya (as of November 2023; Professor, Spain)
Teresa Touriñán (Land Registrar, Spain)

Advisory Committee
Assessors
Matthias Lehmann (Professor, Austria)
Reiner Schulze (Professor, Germany)
Christiane Wendehorst (until September 2021; Professor, Austria)
Aneta Wiewiórowska-Domagalska (Plenipotentiary at Ministry of Justice, Poland)

Other Members
Suzanne Brown Walsh (Attorney, United States of America)
Sergio Cámara Lapuente (Professor, Spain)
José Antonio Castillo Parrilla (Professor, Spain)
José Llopis Benlloch (Notary, Spain)
Peter Lown (Emeritus Professor, Canada)
Donna Molzan (Barrister and Solicitor, Canada)
Sjef van Erp (Sjef van Erp (from September 2022; Emeritus Professor, The Netherlands)
Richard Frimston (Consultant, United Kingdom)

Members Consultative Committee
Individual Members
Sara Adami-Johnson (Wealth Planner, Canada)
Jason Allen (Professor, Australia)
Marina Androulaki (Lawyer, Greece)
Cristina Argelich-Comelles (Professor, Spain)
Alessio Azzutti (Assistant Professor, United Kingdom)
Arvind Babajee (Jurist, Mauritius)
Rosa Giovanna Barresi (Professor, Italy)
Jørgen Bek Weiss Hansen (Attorney, Denmark)
Iryna Dikovska (Professor, Ukraine)

David Dolidze (Professor, Georgia)
Mustafa Ebaid (Researcher, Turkey)
Anh Nguyen (European Law Students' Association Austria)
Laura Maria Franciosi (Professor, Italy)
Muhammed Emirhan Havan (Student, Switzerland)
Gabriela Varia (Professor, Romania)
Habbine Estelle Kim (Lawyer, France)
Alisdair MacPherson (Lecturer, United Kingdom)
Lineke Minkjan (Notary, The Netherlands)
Dimitrios Moustakatos (Lawyer, Greece)
Marlena Pecyna (Professor, Poland)
Meliha Povlakić (Professor, Bosnia and Herzegovina)
Paola Rodas Paredes (lecturer, Spain)
Domenico Rosani (Professor, The Netherlands)
Alina Sarchisian (Lawyer, Romania)
Cécile Sainte-Cluque (Notary, France)
Vyara Savova (Researcher, Bulgaria)
Karen Lynch Shally (Lecturer, Ireland)
Ludovica Sposini (Student, Italy)
Ferenc Szilágyi (Associate Professor, Hungary)
Antonio-Catalin Teodorescu (Student, United Kingdom)
Aura Esther Vilalta Nicuesa (Professor, Spain)
Filippo Zatti (Professor, Italy)
Irina Zlatescu (Professor, Romania)

Institutional Members
Austrian Chamber of Civil Law Notaries (represented by Stephan Matyk-d'Anjony)
Curia of Hungary (represented by Mónika Gáspár; until June 2021)
European Union of Judges in Commercial Matters (represented by Rainer Sedelmayer)
School of Law, University of Hull (represented by Gonzalo Vilalta Puig)
Society of Trust and Estate Practitioners (represented by Leigh Sagar)
University of Latvia (represented by Vadims Mantrov)
Western University 'Vasile Goldis' Arad - Romania, Faculty of Law (represented by Christian Alunaru)

Observers
European Commission (represented by Maria Vilar Badia and Veronica Williams)
Spanish Land Registrars (represented by Silvino Navarro)

ELI Project Officer
Katja Kolman (Project Officer, Austria; until December 2023)
Marta Lages de Almeida (Project Officer, Austria; from March 2024)

List of Abbreviations

ADA	Access to Digital Assets
AML	Anti-Money Laundering
CEPEJ	Commission for the Efficiency of Justice (Council of Europe)
ELI	European Law Institute
EU	European Union
KYC	Know Your Customer
KYBU	Know Your Business User
P&G	Principles and Guidance
Rec (16) 2003	Recommendation No. 16 (2003) of the Committee of Ministers to Member States on the Execution of Administrative and Judicial Decisions in the field of Administrative Law
Rec (17) 2003	Recommendation No. 17 (2003) of the Committee of Ministers to Member States on Enforcement
UIHJ	Union Internationale des Huissiers de Justice (International Union of Judicial Officers)
UNIDROIT	International Institute for the Unification of Private Law

Executive Summary

Digital assets offer new ways of circulating value in modern economies. They have burst onto global markets as a new class of assets for investment, trade, and access to credit. These assets are now held by companies and individuals in their investment portfolios, pledged as collateral in secured transactions to raise funds and access to finance, and transferred across global markets. However, their growing presence worldwide has been accompanied by legal uncertainties and regulatory concerns. On the one hand, their property status has been, and still is, to a certain extent, uncertain, and their legal characterisation varies across jurisdictions. On the other hand, regulators have taken different approaches to activities related to the issuance, transfer, lending or custody of digital assets from the perspective of financial regulation and supervision. Hence, the formulation of harmonised principles and uniform solutions is essential.

Mindful of the need for a harmonised approach to digital assets, in 2019,[1] ELI launched a new project on Access to Digital Assets (ELI ADA project). The project is being developed in different phases. The first phase was marked by the *ELI Principles on the Use of Digital Assets,*[2] which focused on security interests in a digital asset created by a contractual agreement. These Principles were approved by the ELI Membership in February 2022.

In a second phase, the ELI ADA project focused on enforcement against digital assets. As the market for digital assets grows, commercial transactions and also litigation involving digital assets are equally expanding. In such circumstances, creditors, including secured creditors, want to be reassured that they can effectively enforce their rights even when those rights relate to such a new class of assets. Enforcement against digital assets is, in practice, challenged by specific complexities arising from the functional, structural and operational characteristics of digital assets, as well as by uncertainties related to their legal characterisation and regulatory treatment. As a result, enforcement proceedings against digital assets may become more costly, less effective, or even unsuccessful.

These ***ELI Principles and Guidance for Enforcement Against Digital Assets*** hereinafter, the instrument – aim to support courts, lawmakers and international organisations in reforming, adapting, interpreting, or applying rules, procedures, and methods relating to enforcement against digital assets. They also aim to provide legal and practical guidance for enforcement agents, public authorities, (civil law) notaries and commercial arbitrators when facing issues arising from enforcement against digital assets.

A 'digital asset', for the purposes of this instrument, is defined as 'an electronic record that represents a value, a right, or a legally protected interest and which is capable of being subject to control'. This definition is intended to encompass the broadest possible range of digital assets that may be relevant in enforcement proceedings and for enforcement purposes. Digital assets include those representing or recording legally protected interests or rights in other assets, including immovable property. The latter are referred to as 'digital assets linked to other assets'.

Pursuant to the definition of 'enforcement' used in this instrument, self-enforcement and enforcement of security interests in digital assets, unless executed by a public authority, are not covered. However, this instrument can be applied, provided the relevant differences are duly taken into consideration, to identify, access, seize, dispose of, and realise the value of digital assets in insolvency proceedings. It can also serve as guidance in criminal proceedings. Where specific rules exist for enforcement against digital assets in certain regulated sectors, those rules will complement this instrument or prevail over it, resulting in the instrument's modification or replacement.

---

[1] Council Decision CD 2019/4 of 1 March 2019 on the Approval of a New Project on Access to Digital Assets, <https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/eli-enforcement-against-digital-assets/>, accessed on 15 May 2025.

[2] See ELI Principles on the Use of Digital Assets as Security (2022). Available <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf>, accessed on 15 May 2025

As abovementioned, this instrument provides guidance to legislators, regulators, international organisations and others in identifying obstacles that may hamper effective enforcement against digital assets. It proposes a range of policy solutions, from generous interpretations of existing concepts and rules to include digital assets, to the specification and clarification of their property status and/or recognition as enforceable assets through legal reform or judicial decisions. In developing their own solutions, States are encouraged to recognise the global dimensions and impact of digital assets, and the importance of cross-border cooperation. While harmonisation of substantive rules is primarily encouraged, international cooperation to establish uniform conflict-of-law rules is also essential, and is recommended.

Although this instrument covers digital assets linked to other assets, it does not aim to alter the rules governing the transfer of those underlying assets, in particular immovable property, in accordance with the applicable law. However, as there is an interplay between the rules governing the transfer of such digital assets and its effects and the rules governing the transfer of the underlying asset, this instrument encourages States to carefully analyse this interplay and explore and consider possible solutions, including law reform and the implementation of innovative solutions.

The debtor's cooperation and that of third parties is highly relevant for effective enforcement. Therefore, this instrument provides guidance in relation to disclosure obligations, search measures, access to information, and access to digital assets, which includes actual attachment and the effective seizure of digital assets.

This instrument is designed to be adaptable to any enforcement model in a jurisdiction, regardless of its structure or type of enforcement agents involved. 'Enforcement agents' is used as a neutral concept that can be adapted to the model applicable in each jurisdiction (eg private, self-employed, court or public). While general enforcement rules should apply to digital assets, where needed, specific enforcement rules and procedures, should also apply. Legal measures as well as technological tools (such as a designated wallet for digital assets) are proposed to enable the control, custody, and seizure of digital assets by enforcement agents. Likewise, valuation criteria and realisation methods, including transfer as payment to the creditor, need to be adapted to digital assets.

Since the project's inception, several organisations, institutions, and authorities have focused their attention on various aspects of digital assets, resulting in the formulation of principles or rules for the crypto market or crypto-related activities. Court decisions worldwide are beginning to address issues related to enforcement against digital assets in a variety of situations and contexts. These projects and initiatives, along with their initial[3] and final outcomes (see Sources), as well as changes in the law, were carefully considered in ELI's broader ADA project and, in particular, during the second phase which focused on enforcement against such assets. This is intended to ensure that the project contributes to the global debate and adds value by providing additional guidance.

The proposals put forward below result from a culmination of discussions with the Project Team, Advisory Committee, Members of the Consultative Committee, Project Observers and ELI's Scientific Director.

The resulting instrument is structured on two levels: Principles and Guidance to Implementation

(hereinafter, **P&G**).

[3] International Institute for the Unification of Private Law (UNIDROIT) Working Group on Best Practices for Effective Enforcement. For information on this project, and on the members and observers of the Working Group, see <https://www.unidroit.org/work-in-progress/enforcement-best-practices/>, accessed on 15 May 2025.

General Provisions

A. Structure and aim of the instrument

1. This instrument aims at providing guidance to courts, lawmakers and international organisations in reforming, adapting, interpreting, or applying enforcement rules, procedures, and methods as regards enforcement against digital assets. This instrument also contains legal and practical guidelines that may be used by enforcement agents, public authorities, (civil law) notaries and commercial arbitrators faced with issues relating to enforcement involving digital assets.

2. This instrument is structured on two levels: Principles and Guidance (P&G). Each of the ten Principles below is accompanied by Guidance that elaborates on the Principle or addresses specific issues related to it, to assist in its application, interpretation, or incorporation into domestic laws or supranational instruments.

B. Definitions

1. For the purposes of these P&G, a 'digital asset' is an electronic record that represents a value, a right, or a legally protected interest and which is capable of being subject to control.[4]

   Digital assets falling under these P&G include those that represent or record legally protected interests or rights in other assets, whether tangible or intangible. These digital assets are referred to as 'digital assets linked to other assets'.[5] The asset that a 'digital asset linked to other assets' represents or is linked to is referred to as the 'underlying asset'.

2. For the purposes of these P&G, 'enforcement' comprises procedures carried out by a public authority or under the supervision (or authorisation) of a public authority, through which a claimant, including a secured creditor, can obtain satisfaction of their claim against a debtor, by means of the enforcement of a court decision, an enforceable arbitral award, an out-of-court settlement or another enforceable instrument, as defined by the applicable law, as far as these procedures involve enforcement against digital assets.

3. For the purposes of these P&G, the term 'third parties' globally refers to any provider of services related to digital assets whose cooperation may be required for enforcement purposes, such as providing relevant information, or performing one or more actions aimed at cooperating in searching, or disclosing assets, preventing dissipation (complying with freezing orders, blocking or suspending access), transferring or seizing assets.

C. Scope

1. These P&G apply to enforcement against digital assets, as defined in this instrument (*supra* B.1.).

---

[4] As explained under C.1. below, these P&G depart from the definition of digital assets used in the ELI Principles on the Use of Digital Assets as Security, with the sole aim of better accommodating the definition to the scope and purpose of this instrument (enforcement) by employing a broad definition. The definition used in these P&G encompasses the definition of digital assets used in the ELI Principles on the Use of Digital Assets as Security and is aligned with the definitions used in other international instruments, such as the UNIDROIT Principles on Digital Assets and Private Law (2023), Principle 2, <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>, accessed on 15 May 2025. Or more generally the UNCITRAL texts on e-commerce and electronic transferable records, <https://uncitral.un.org/en/texts/ecommerce> (namely, the notions of electronic record, or control).

[5] Reference is here made to 'digital assets representing real-world assets' in the ELI Principles on the Use of Digital Assets as Security (2022), available <https://www.europeanlawinstitute.eu/projects-publications/publications/eli-principles-on-the-use-of-digital-assets-as-security/> accessed on 15 May 2025. UNIDROIT Digital Assets and Private Law Principles refer to 'linked assets' (Principle 4), <https://www.unidroit.org/instruments/digital-assets-and-private-law/> accessed on 15 May 2025.

Thus, the definition of digital assets in this instrument departs from the definition used in the first part of the ELI project on the Use of Digital Assets as Security,[6] considering that the P&G have been drafted for the specific purposes of enforcement. Therefore, the definition of digital assets has been drafted accordingly, and with the aim of covering as broad a range of digital assets as possible that may be relevant in enforcement proceedings and for enforcement purposes.

These include assets linked to other assets, as defined in this instrument (*supra* B1), including those digital assets linked to immovable property. However, it is not the aim of these P&G to affect the applicable law governing the transfer of immovable property. Any transfer of a digital asset linked to other assets, including immovable property, will be subject to the law applicable to the underlying asset (immovable property).

2. These P&G do not prejudge the enforcement model in force in a jurisdiction, whether in terms of organisation, structure, or the type of enforcement agents involved (private/self-employed or public, such as civil servants). Each jurisdiction may incorporate these P&G into its enforcement framework with the required adjustments depending on its specific structures, organisational set-up, and governance. These P&G generally refer to 'enforcement agents' as a neutral concept that can be adapted to the model applicable in each jurisdiction.

   The enforcement of security rights in digital assets, unless executed by a public authority, is not covered by these P&G.[7]

   Accordingly, and given the definition of 'enforcement' for the purposes of this instrument (*supra* B.2.), these P&G do not apply to self-enforcement mechanisms that parties may agree upon in the event of default and that operate as defined by the parties in an agreement ('agreed consequences in event of default').[8]

3. As a principle, the general rules on third parties in enforcement proceedings also apply to third parties as defined in these P&G (*supra* B.3.). However, not all third parties are in a position to perform these actions. Therefore, where necessary, these P&G may refer to a class or classes of third parties specifically in relation to certain obligations. For enforcement purposes, cooperation is then requested or provided to a specific third party under enforcement law, and not to any third party simply because it provides services related to digital assets.

4. Where relevant, these P&G may apply to identifying, accessing, seizing, disposing of, and realising the value of digital assets in insolvency proceedings. However, these P&G do not contain any specific rules on insolvency matters.

5. Only to the extent that these P&G apply to identifying, accessing, seizing, disposing of, and realising the value of digital assets do they serve as guidance for addressing these issues in criminal proceedings, taking into consideration the relevant differences between criminal and civil proceedings.

6. When applying these P&G, specific regulations for enforcing digital assets in certain sectors, in particular, regulated ones such as financial markets, should be acknowledged and properly considered. If such regulations exist, they complement, modify, or replace these P&G.

---

[6] Reference is here made to the ELI Principles on the Use of Digital Assets as Security (2022), <https://www.europeanlawinstitute.eu/projects-publications/publications/eli-principles-on-the-use-of-digital-assets-as-security/> accessed on 15 May 2025.

[7] Reference is here made to the ELI Principles on the Use of Digital Assets as Security (2022), available <https://www.europeanlawinstitute.eu/projects-publications/publications/eli-principles-on-the-use-of-digital-assets-as-security/> accessed on 15 May 2025.

[8] Reference is here made to the ELI Principles on Blockchain Technologies, Smart Contracts and Consumer Protection (2023).Available <https://www.europeanlawinstitute.eu/projects-publications/publications/eli-principles-on-blockchain-technology-smart-contracts-and-consumer-protection/>, accessed on 15 May 2025. .

Principles and Guidance

Principle 1: Enforcement against digital assets

1. Enforcement should not be denied solely on the grounds that the assets enforced against include or comprise digital assets.

2. Digital assets are subject to enforcement to the extent that they hold value relevant to the proceedings.

Guidance to Principle 1

a) The uncertain property status of digital assets may hamper effective enforcement: hence, clarifying their status for enforcement purposes is strongly recommended.

States should consider whether enforcement difficulties arise from uncertainties as to the property status of digital assets and take appropriate action to provide legal certainty. The intangible, incorporeal, and digital nature of digital assets may lead to difficulties in qualifying such assets as property in some jurisdictions. Consequently, subsequent effects on enforcement can follow. Clarifying the property status of digital assets would remove obstacles to enforcement, eliminating the need to specify or clarify their enforceability as outlined in paragraph b) below. Each State should assess the sufficiency and the adequacy of the different solutions – as laid down in a) and b) – within the context of its relevant legal system.

b) Without prejudice to paragraph a) above, a clear legal recognition of digital assets as assets susceptible to enforcement is advisable as it would provide a stronger legal basis for enforcement law to effectively apply to digital assets.

States should consider whether the notion of assets under enforcement law or for enforcement purposes sufficiently covers digital assets or certain subclasses of digital assets, as well as take steps to provide legal clarity.

States can explore different possible options and choose the one most adequate to their jurisdiction. First, they may reform the law to explicitly recognise digital assets as enforceable assets, either through general legislation or specific provisions in procedural laws. Second, guidance encouraging a broad interpretation of 'assets', embracing digital assets, for enforcement purposes, could be provided. This could help clarify the issue for courts and remove obstacles to enforcement, even without formal statutory recognition.

c) The digital characteristic of assets should not prevent parties from enforcing their rights under enforcement law, on terms equivalent to other assets, unless the State imposes bans, limitations, or restrictions on enforcement against certain assets on other grounds (see Principle 4). In such cases, these bans, limitations or restrictions should apply to digital assets in the same manner as they apply to such equivalent assets.

States should avoid implementing such bans, limitations or restrictions on enforcement solely based on the digital character of assets, as that may, on the one hand, lead to unjustifiably differentiated treatment between claimants, to the detriment of parties involved in transactions with digital assets; and, on the other hand, interfere in market dynamics. This would discourage the issuance and the transfer of certain classes of assets (digital assets) and stifle innovation in business models or transactions based on, or driven by, digital assets. Should States consider interference necessary on policy grounds, alternative regulatory or normative solutions may be more effective, predictable and legally certain. If only digital assets are targeted, parties who have already concluded transactions in accordance with the law could see their interests and expectations frustrated, especially during critical situations, such as in the case of default or insolvency.

d) For enforcement purposes, claimants should consider whether digital assets have value

that can achieve enforcement goals and satisfy their interests. This assessment should take into consideration the type of claims, including monetary and non-monetary claims.

Where enforcement aims to recover a monetary value, it should be considered whether third parties can take control of, or transfer, the digital assets in exchange for payment.

e) States should be mindful that courts and enforcement agents also face difficulties as regards enforcement because they may be unfamiliar with digital assets, or lack effective technological, contractual, and procedural tools or frameworks to address them. Irrespective of whether the enforcement system is private or public, States should provide a suitable environment and deploy the necessary infrastructure for enforcement against digital assets, which includes:

e.1. enacting, reforming, or applying enabling legislation aligned with international standards, and, in particular, these P&G;

e.2. ensuring that the authority, jurisdiction, and powers of enforcement organs are adequate and sufficient to achieve effective enforcement against digital assets, considering their characteristics;

e.3. implementing training programmes for courts, enforcement agents and other authorities involved in any activity related to enforcement against digital assets, to enhance their familiarity with digital asset classes, practices, technological features, and their operation;

e.4. deploying an interoperable and interconnected infrastructure of registers and databases relevant for accessing information, tracing, or taking control of digital assets for enforcement purposes, and, where necessary and in accordance with proportionality criteria, ensuring ready access for enforcement agents for the specific purpose of enforcement against digital assets; and

e.5. facilitating the implementation of technological solutions to make enforcement actions feasible and effective (such as special wallets pursuant to Principle 9 and the corresponding Guidance in these P&G).

Principle 2: General and specific enforcement provisions

1. General enforcement provisions should apply to enforcement against digital assets to the greatest extent possible, insofar as the application is feasible, given the functional, operational and substantive characteristics of digital assets.

2. Enforcement against digital assets must comply with any special provisions or enforcement rules applicable to specific types, or classes of assets, where the digital asset being enforced against is similar or analogous to those specific types or classes of assets to which the special provisions or rules apply.

   In particular, formalities and other requirements for enforcing such assets should not be waived solely on the grounds that enforcement is against digital assets.

3. Specific provisions for the enforcement against digital assets should be applied only when necessary and based on the unique functional, operational, or substantive characteristics of digital assets.

Guidance to Principle 2

a) Generally, special enforcement procedures for digital assets, separate from current general enforcement procedures or those available for specific classes of assets, do not appear necessary nor advisable. General enforcement rules should apply to digital assets, with specific enforcement rules, procedures or methods for subclasses of digital assets, when necessary.

Specific enforcement rules, procedures or methods may be established by law for securities or other financial instruments in general. These rules, procedures or methods should also apply to enforcement of digital assets classes that are treated as, or assimilated to, securities in particular, or financial instruments in general.

b) If States adopt specific enforcement rules for digital assets – or one or several subclasses – on the sole basis of their digital nature, the scope of application should be clearly defined to avoid uncertainties or overlaps, accommodate technological progress, and prevent parties from opportunistically evading the rules in substantially equivalent cases.

c) States can create specific laws or encourage the use of analogies based on functional equivalence to determine whether rules specific to certain types or classes of assets, including rules on formalities and other requirements, apply to particular types or classes of digital assets. In doing so, States should consider the need for certainty and technology neutrality as well as the ability of their legal framework to adjust to future changes. Nonetheless, in some legal systems, the use of analogy may be very limited in procedural law, and authorities may not be familiar with the principle of functional equivalence. In such cases, it may be necessary to create special enforcement rules for digital assets or, more adequately, it may be deemed convenient to explicitly specify that general or specific enforcement rules, while applicable to assets other than digital assets, also apply to enforcement against one or several types or classes of digital assets.

Principle 3: Legal nature/characterisation and global aspects

1. These Principles do not prejudge the legal nature of digital assets for enforcement purposes.

2. The *lex fori* will determine the legal nature of the digital asset for the purposes of the enforcement proceedings.

   When dealing with digital assets linked to another asset (an underlying asset), the legal characterisation of the digital asset will be determined in accordance with Principle 5.

3. Considering the global nature of the digital assets market, States should cooperate to develop internationally harmonised solutions, and make best efforts to coordinate regulation and enforcement against digital assets.

Guidance to Principle 3

a) Pursuant to the Guidance to Principle 1, States should reduce uncertainty by clarifying the legal characterisation and property status of digital assets.

   States should be mindful that lack of certainty in *lex fori* would lead to inefficiencies, such as the non-enforcement of orders, an unappealing forum for digital assets, competitive disadvantages globally, and opportunities for arbitrage and forum shopping.

b) States should recognise that digital assets have a global dimension and impact. Therefore, they should be willing to develop international instruments and agree on harmonised rules. A solely domestic approach to digital assets is not advisable, as it contradicts the decentralised, international, and delocalised operation of the market.

   As *lex fori* applies to determine the legal nature of digital assets, substantially diverging approaches in national laws lead to uncertainties and market fragmentation. Therefore, adopting unified rules for digital assets appears to be the optimal solution. However, due to sensitivities surrounding State sovereignty in property law, among other fields, achieving legal consensus can be challenging. Consequentially, States should explore other forms of harmonisation to address divergences in the treatment of digital assets, particularly in the area of enforcement. Pragmatic solutions – aimed at effectively fulfilling core enforcement purposes – that move beyond classical dogmatic asset characterisation may be advisable to avoid frustration of expectations, reduce legal uncertainty and

safeguard the economic interests of parties involved.

c) In particular, States should be mindful that, considering the global nature of digital assets, the recognition of foreign enforcement instruments/documents is crucial for effective enforcement. Different approaches and interpretations of the concept and legal nature of digital assets create problems in recognising and enforcing orders, rendering the process complicated and expensive. To address this, there should be increased focus on enhancing knowledge in foreign enforcement systems.

d) At a minimum, States should strive to follow uniform standards and contribute to harmonisation in the field of digital assets through domestic initiatives. Additionally, States should consider the following:

d.1. Clear, highly harmonised provisions on applicable law and jurisdiction are essential for effective enforcement of digital assets. Ambiguities create complexities. Given the internationality and decentralisation features of digital assets, States should cooperate to the greatest extent possible to reduce uncertainties, and enhance predictability with the adoption of common or harmonised conflict-of-law rules and jurisdiction rules.

d.2. Clear rules on the jurisdiction of enforcement agents should be established. Considering the decentralised nature, digital format, and absence of a 'location', in a traditional geographical sense, of digital assets, enforcement agents should be empowered to take effective measures to access digital assets for enforcement purposes.

d.3. Measures to ensure effective access to digital assets in a jurisdiction other than where the enforcement proceeding is taking place should be established under the applicable law. Otherwise, enforcement will often be severely limited or compromised.

Principle 4: Proportionality and adequacy

The choice of enforcement measures against digital assets should be appropriate to the interests of the parties involved, the value of the claim, the value of the digital assets, the effectiveness of general enforcement measures, or specific measures if available, and the urgency of the case.

Guidance to Principle 4

a) The enforcement measure should be proportional to the amount of the claim. During the enforcement process, enforcement agents should choose the least limiting or invasive option, taking into consideration the amount of the claim, the duration, nature and costs of enforcement. To achieve a fair balance for the parties, enforcement agents should be able to adapt the measures to the specific circumstances and take appropriate action to protect the interests of all parties involved.

b) Any restrictions or limitations to, or exemptions from, enforcement against certain assets, asset values or classes of assets (such as assets necessary for the subsistence of the debtor and their family, maintaining basic domestic needs and human dignity, and for business, profession or employment) should apply under equivalent conditions to enforcement against digital assets.

Principle 5: Digital assets linked to other assets

1. If a digital asset is linked to another asset, whether tangible or intangible, the existence of that link, the prerequisites for establishing such link, and its legal effects are to be determined by the law applicable to the asset that the digital asset represents or is linked to (the 'underlying asset').

2. The legal effects of enforcing against the digital asset, as they relate to the underlying asset, should be determined by the law applicable to the underlying asset, as determined by the ordinary conflict-of-laws rules. In the event of conflict, that law prevails.

3. Where the link has been established through the registration of the asset in a public registry, the relevant requirements, effects and enforcement rules shall be made in accordance with the conflict-of-law rules applicable to the publicity of assets (*lex registrationis*).

Guidance to Principle 5

a) Conflict-of-laws rules should be clear and apply to digital assets linked to other assets, as suggested in Principle 5(1). Any uncertainties in their interpretation and application should be minimised.

b) Pursuant to Principle 3, while harmonisation of substantive rules is primarily encouraged, international cooperation to establish uniform conflict-of-law rules for digital assets linked to other assets is also essential to directly or indirectly minimise substantive legal disparity.

c) As digital assets linked to other assets also include those linked to immovable assets, States should carefully consider the interplay between the rules governing the transfer of such digital assets and their effects and the rules governing the transfer of the underlying asset pursuant to the applicable law. These P&G do not aim to alter or in any way affect the rules governing the transfer of immovable property law solely on the ground that digital assets linked to such immovable property are issued and transferred.

Where digital assets are linked to immovable property, States should, however, analyse current rules governing the transfer of immovable property, and, if necessary, consider their reform or innovative solutions, such as enhancing real estate market liquidity, attracting investment, or facilitating affordable access to housing in certain circumstances, to achieve policy goals.

These P&G do not suggest that the transfer of a digital asset linked to immovable property suffices to comply with the requirements for the transfer of title to immovable property. Each State should assess how the transfer of digital assets linked to immovable property interacts with the existing rules governing the transfer of immovable property. To that end, the following steps should be considered.

First, it should be noted that digital assets linked to immovables can represent different interests or rights related to immovable property. Some digital assets represent 'property rights' in the immovable asset, while others represent related rights, such as security interests or contractual rights (such as rent agreements, or investment agreements). These digital assets are significantly different in terms of their legal nature and their transfer will have different legal effects depending on the right or interest they represent.

Second, considering the foregoing, when the digital asset represents a proprietary right related to an immovable asset, each State should carefully assess how the digital asset's representation of that right and its subsequent transfer interact with the rules applicable to the transfer of immovable property. For instance, the transfer of the digital asset could be interpreted as mere documentary evidence of the agreement between the parties or be deemed as fulfilling certain requirements of the law applicable to conveyance (*traditio ficta*).

Third, States might wish to explore the development and the implementation of innovative solutions to bridge the market between digital assets and the real estate market in an effective way. Solutions could be aimed at connecting trading venues or platforms for digital assets with land registries to record the transfer and ensure consistency or at finding technical solutions to give access to registers containing information about digital assets or the assets themselves, granting full legal effects to the transfer upon registration. Other solutions, dependent upon each State's applicable law and registry model, may be explored.

Such analysis and possible solutions directly impact enforcement against digital assets linked to immovable property, determining the effectiveness of such enforcement, and its legal effect on the underlying asset.

Principle 6: Disclosure obligations

1. The debtor has a primary duty to cooperate in providing information to identify or locate the digital assets, facilitating access to devices or systems, and enabling disposition, transfer or seizure of digital assets to ensure effective enforcement.

2. Enforcement laws should include measures to compel the debtor to disclose information regarding their digital assets and provide the necessary details to locate them for enforcement purposes. Pursuant to paragraph 4 below, the law of the debtor's residence or place of establishment governs these measures or any restrictions on the disclosure obligation.

3. If the debtor refuses to cooperate, or cannot effectively provide the requested information, third parties should be approached to obtain information about the identity of the asset holder, the debtor's account, the digital assets, or other details relevant for tracing and/or locating them.

4. The adoption, the extent, and the enforceability of measures to compel the debtor and/or third parties to cooperate in the enforcement of digital assets should be subject to the law of the State where such parties have their habitual residence or place of establishment.

5. If the debtor or any third party refuse to cooperate without any legitimate reason, including by intentionally/(grossly) negligently providing incorrect, misleading or false information, enforcement law should provide for adequate and proportionate consequences.

6. Limitation periods should not apply to enforcement if digital assets are not disclosed by the debtor or any third party when compelled to do so during the enforcement proceedings pursuant to the previous paragraphs.

Guidance to Principle 6

The obligations of the debtor

a) For an efficient enforcement system, it is important that the search for, and seizure of, the debtor's assets is carried out as effectively as possible. International standards refer to a fast and efficient collection of information on assets. This means that either the creditor, who is expected to propose the means and objects of enforcement, or the enforcement agent should have access to relevant information about such assets from official registers or other sources. International principles also impose a duty on parties to cooperate appropriately in the enforcement process, with the debtor being obliged to provide up-to-date information on their income, assets and other relevant matters.[9]

To facilitate the search for assets, many countries have introduced a requirement for the debtor to submit a statement of assets. In response to such a request, a court or enforcement agent may even seek information from third parties. Debtors and third parties may be fined for lack of cooperation or held liable for providing false statements.

b) States should be mindful that effective cooperation of the debtor and third parties is decisive or highly critical for the effectiveness of digital assets' enforcement. Enforcement rules and measures should be tailored to that end,

[9] See Council of Europe Recommendation Rec (2003)17 of 9 September 2003 under III1c and d e and III26. Also, Article 83 UIHJ Global Code on Enforcement.

considering the characteristics of digital assets and the roles of third parties involved in their enforcement.

In accordance with Principle 6(2) and (4), the adoption, the scope, and the enforceability of measures to compel the debtor and/or third parties to cooperate in the enforcement of digital assets should be subject to the law of the State of such parties' habitual residence or place of establishment. This is the most common and accepted solution at present. However, considering the global character and delocalised nature of digital assets, enforcement proceedings against, or involving, digital assets often affect or involve multiple jurisdictions.

Hence, deferring to the law of the residence or place of establishment of the relevant parties compelled to cooperate for the purposes of disclosure may lead to inefficiencies that hinder enforcement. Therefore, States are encouraged to cooperate in revising applicable laws to facilitate full access to information across jurisdictions.

Third parties

c) Existing enforcement laws already establish cooperation duties for third parties. In the context of enforcement against digital assets, additional (non-traditional) third parties – such as custodians,[10] venue trading operators, wallet service providers, registry entities, as defined above (B.3 above) for the purposes of these P&G – may also be considered for cooperation.

Some intermediaries may be traditional financial intermediaries, while other third parties providing services related to digital assets – such as custodians, wallet service providers, registry entities, venue trading operators – are not. States may regulate these (crypto) intermediaries through bespoke regulations.[11]

These regulations should provide for rules that directly or indirectly (such as the 'Travel Rule' mandates intermediaries to share certain information about the originator and beneficiary of transfer) enable enforcement by facilitating cooperation for enforcement purposes. Clear legal bases are needed to serve these intermediaries and instruct them on their obligations to cooperate. Rules should be adapted accordingly if necessary.

In particular, requests for information to be provided by third parties should adhere to the following conditions:

c.1. Third parties should be informed of the penalties for refusal to report or for incomplete or false reporting.

c.2. Third parties should be required to provide a list of the debtor's digital assets.

c.3. Third parties should be informed of the timeframe within which the required information must be provided, or, if necessary, be granted a reasonable period of time for compliance.

Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations[12] provide for duties and obligations that may be crucial for tracing and locating digital assets for enforcement purposes. These regulations may be applicable, in certain jurisdictions, only to traditional financial intermediaries (including

[10] As defined by the UNIDROIT Principles on Digital Assets and Private Law. Custodian is a term that has different meanings depending on the jurisdiction and the field of law. Thus, for the purposes of these P&G, the concept is defined in relation to services provided in relation to a digital asset under a custody agreement pursuant to UNIDROIT Principles on Digital Assets and Private Law, Principle 10.

[11] 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.

[12] For example, Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, as modified in July 2024.

payment service providers), while in other jurisdictions, they may have been modified to explicitly include or cover crypto intermediaries[13] (third parties for the purposes of P&G).

States should revise their regulations on these matters and assess whether they sufficiently cover third parties in relation to digital assets, insofar as KYC/AML tools can be of utmost relevance for enforcement against digital assets.

Besides, specific types of crypto intermediaries (but not all third parties for the purposes of these P&G) can be subject to special duties pursuant to crypto-specific regulations.[14]

Other provisions applicable to digital intermediaries (platform operators, digital service providers), but not related to crypto markets, may provide for measures and tools enabling enforcement. Know-Your-Business-User (KYBU) obligations and traceability duties[15] may help in the identification of the debtor.

Considering the foregoing, and without prejudice to the above-referred regulations, for taxation purposes, anti-money laundering or other public interest purposes, States should consider imposing a duty on any intermediaries engaged in activities related to digital assets (third parties for the purposes of these P&G) to inform, cooperate, and decide on the scope and the conditions of this duty.

Sanctions

d) A non-cooperative debtor or third party should be sanctioned. However, sanctions for non-compliance with enforcement orders (coercive fines, coercive detention) are not always effective in compelling such cooperation. A reconsideration of systems of sanctions, other than fines or penalties, such as a temporary withdrawal of a passport or driving licence or civil imprisonment, may prove more efficient or practically have a more deterrent effect.

e) Existing legislative restrictions on the application of certain sanctions should be identified and removed. For example, a fine, though most common, is not permissible in all countries if the enforcement claim relates to a monetary claim.[16]

Limitation periods

f) Where limitation periods are provided for by national legislation, the effectiveness of enforcement can be undermined if digital assets are not disclosed by the debtor or by any third party compelled to do so during enforcement proceedings. Delayed disclosure can lead to the application of limitation periods, and hinder enforcement. Therefore, alongside effective disclosure mechanisms, provisions exempting the application of limitation periods in such circumstances should be incorporated into applicable law.

Principle 7: Search measures and access to information

1. Mechanisms established to obtain information, to access and search the debtor's assets, including digital devices, systems, and accounts, should be proportionate and effective.

[13] For instance, 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.
[14] 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.
[15] Such as Article 30 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).
[16] For example, the Benelux Agreement on the Uniform Law on Penalty Payments (26 November 1973) does not allow a penalty for monetary claims.

2. Where multiple mechanisms are available, the chosen method should consider, among other factors, the risks to privacy, trade secrets and confidential information exposure, as well as the effectiveness and suitability of the mechanisms in the particular context of digital assets, considering their functional, operational, and substantive characteristics.

3. Enforcement agents should be authorised, when necessary for the enforcement, to request access to relevant information on the debtors' digital assets or related transactions from competent authorities, even if such information was provided or collected for other purposes.

Guidance to Principle 7

a) The importance of access to information on the domicile and (digital) assets of a debtor is recognised in international standards.[17]

Within Europe, the Council of Europe's Commission for the Efficiency of Justice (CEPEJ) recommends the establishment of a unique multi-source restricted access database on a debtor's attachable assets.[18] The development of such a database, in the view of the CEPEJ, will require co-operation between the various organs of State and private institutions, subject to compliance with data protection legislation.[19]

To facilitate efficient enforcement, the CEPEJ 2009 Guidelines further recommend imposing an obligation on State authorities which administer databases required for efficient enforcement to provide information to enforcement agents.[20]

These P&G further recommend that national legislation be reviewed to assess if adaptations would streamline enforcement procedures.[21]

The necessity for legal provisions

b) In most European countries, a system for accessing information on the assets of a debtor exists and is largely automated. In most States, such access also relates to non-public databases.

At the same time, it is to be noted that access to information on the bank account(s) of a debtor is rather limited. The same applies to information from tax authorities. In the case of self-employed (private) enforcement agents, only a few countries allow access to information from the tax authorities.

Such limitations will hinder efficient enforcement. Taking into consideration the particularities of digital assets, the current legal provisions on access to information might be insufficient. States should also consider the possibility of enforcement agents having access to available information on digital assets that has been collected for specific purposes. In particular, but not exclusively, information provided to tax authorities for taxation purposes, and information related to parties and transactions on digital assets provided to competent authorities in compliance with anti-money laundering, and terrorism financing. To that end, specific authorising rules for enforcement agents for these purposes should be adopted or clarified.

c) Clarity on the role of enforcement agents in their search for digital assets should be provided. This includes access to the digital devices, systems or accounts of the debtor to identify, locate or trace digital assets. Clear and specific rules and practices should be provided for enforcement agents to access, seize, or search technological

[17] See, for example, Council of Europe Rec 17/2003 under III.6 and CEPEJ Guidelines 2009 under 39 and 47.
[18] CEPEJ 2009 Guidelines under 41.
[19] CEPEJ 2009 Guidelines under 42.
[20] CEPEJ 2009 Guidelines under 43.
[21] CEPEJ 2009 Guidelines under 44.

devices – either requiring the physical seizure of the device or remote access to digital systems by logging into and accessing a debtor's accounts.

Expert assistance

d) The enforcement agent might not have the technical knowledge to examine digital devices to identify digital assets. It should be possible that the enforcement agent is assisted by a computer expert to examine such digital devices.

The role of such experts in searching for digital assets is relevant and should be contemplated in the law and clearly defined. Clear rules on the selection and appointment of these experts, allocation of costs, and duties should be provided. General rules for experts in enforcement laws would suffice, unless special consideration of their duties and tasks in relation to digital assets is expected and require specific consideration. Confidentiality obligations should be clearly determined and should apply to such experts. In most jurisdictions, such rules are included in conduct rules for enforcement agents.

Data protection

e) Data protection and privacy rules are particularly relevant in searching for digital assets.

Data protection duties should clearly apply to enforcement agents. Enforcement agents and experts involved in the search for digital assets are responsible for maintaining confidentiality when confidential, sensitive or secret information comes to their attention. Any breach of such duties should result in disciplinary, civil or criminal liability.

Cybersecurity

f) Cybersecurity risks may arise during search activities. Enforcement agents should be trained to understand and handle these risks and be able to prevent and mitigate them.

International cooperation

g) Digital assets, by their nature, are not restricted by geographical borders. States may consider the development of a mechanism for cooperation between (enforcement) authorities to enable rapid access to information about a debtor's digital assets in another State.

A similar cooperation can be found in Regulation (EU) No 655/2014 of the European Parliament and of the Council of 15 May 2014 establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery in civil and commercial matters. This Regulation provides, in Article 14, that a creditor may obtain information about the bank account of a debtor to enforce a preservation order. The court to which the request for a preservation order is made must transmit the request for information to the authority in the addressee Member State responsible for requesting information. The national law of each Member State must provide for methods of obtaining information, particularly by requiring the banks within their territory to declare whether the debtor has an account and to disclose such details to the person responsible for collecting the information (Article 14).

Principle 8: Access to digital assets

1. For the purposes of this Principle, access to digital assets is understood to enable the actual attachment and effective seizure of the accessed digital asset.

2. Only enforcement agents authorised by national law, regardless of their status, should have the authority to access a person's digital assets for the purpose of executing an enforceable title/instrument/document recognised by the applicable law.

3. Adequate measures, such as interim relief or other orders under the applicable law, should be available to prevent the dissipation of digital assets before enforcement is completed, ensuring effective enforcement.

4. When digital assets are recorded in public registries, necessary measures must be taken

to ensure that enforcement is effective against third parties, through appropriate notations or registrations in the relevant registry.

Guidance to Principle 8

a) To effectively access digital assets, consideration should be given to different holding models and the role of relevant third parties. Accordingly, enforcement agents should be authorised by applicable law to request information from the debtor or from third parties (in the sense that these P&G use the term, such as custodians, providers, where applicable and to the extent that it is relevant for the envisaged action) to access digital assets; retrieve information from devices, systems, or accounts; and instruct custodians to transfer digital assets, when necessary, for enforcement purposes.

Access to digital assets held by the debtor

b) Should digital assets be held by the debtor (such as in cold wallets, or web wallets), enforcement agents should be authorised under the applicable law of the debtor's residence or place of establishment to gain access to the private key stored in the wallet. If the debtor does not voluntarily cooperate, the device would have to be seized and/or access to the system or account where the private key is available would have to be gained. Enforcement agents should be authorised by applicable law to take adequate measures to decipher, access, log in, or by any other means, act in place of the debtor to access their digital assets.

Enforcement law should provide that enforcement agents may be assisted by IT or technical experts, when necessary, to perform such actions.

Similar concerns to those expressed previously in relation to diverging national laws of the debtor or third parties in relation to the duty to disclose, apply here. States are invited to assess whether diverging national laws create obstacles for enforcement agents to effectively gain access to private keys in multiple-jurisdiction enforcement proceedings.

Access to digital assets held by a custodian

c) Should digital assets be held by a custodian (a third party for the purposes of these P&G), enforcement agents should be authorised by applicable law to request the custodian to provide a debtor's login credentials or otherwise gain access to a debtor's account for the sole purpose of accessing their digital assets.

Upon being served, the custodian should be given a reasonable period of time, defined by applicable law, to notify enforcement agents as to whether or not they hold digital assets for the debtor's account under penalty defined by the applicable law. The custodian should be informed of the penalties for refusal to report or for incomplete or false reporting.

The custodian should be required to provide a list of digital assets, as well as their access codes (public key, private key) in a way that enables their seizure.

The custodian should be required to declare any previous seizures or security interests or guarantees on the digital assets under penalty defined by the applicable law.

Enforcement agents should also be authorised to instruct custodians holding digital assets on behalf of the debtor to transfer relevant digital assets to comply with the enforcement title/instrument/document.

Principle 9: Designated wallet for digital assets of enforcement agents

1. Enforcement authorities should implement technological solutions to enable the seizure of digital assets and an appropriate custody for the sole purposes of enforcement.

2. In particular, designated wallets under the authority of the enforcement agents should be made available.

Guidance to Principle 9

The principle of the designated wallet

a) Some jurisdictions, in particular European countries, have introduced, in accordance with international standards,[22] the designated bank account, in which the money received within the enforcement proceedings is to be deposited. A separate account is maintained by the enforcement agent for and the reimbursement of enforcement costs, the performance fee and the expenses incurred by additional activities. Such a designated bank account is solely used for:

a.1. Payment of creditors from the amounts collected on their behalf through enforcement actions.

a.2. Payment for the costs of enforcement actions and for ensuring their efficiency.

a.3. Payment to the debtor of the amount outstanding upon full payment of the creditor and of the respective fees for the enforcement agent.

Such a designated bank account was introduced to safeguard the interests of creditors and debtors. The enforcement agent only administers the account but does not own it. The rights to the funds are held jointly with the rightful creditors.

The enforcement agent is exclusively authorised to access and approve payments from the designated bank account. They remain responsible for all transactions to and from the designated bank account. The enforcement agent must maintain a record of all entries and withdrawals, including transaction amounts, dates, numbers of cases for which transactions are made, and the full names of each depositor and recipient of payments.

Current legislation could also apply *mutatis mutandis* to introduce designated wallets for digital assets. Enforcement agents could maintain at least one designated wallet, used solely for digital assets resulting from enforcement, and should manage it in conformity with the diligence standards applicable to their profession.

Digital assets stored in the designated wallet may not be the subject of seizure for the purpose of settling any debts of the enforcement agent. As is the case with the designated bank account, the right of all claimants whose funds are stored in the designated wallet is to be calculated on a pro rata basis, in accordance with the amount that has been paid into the designated account for their benefit. Adequate training should be provided to enforcement agents managing the wallets for enforcement purposes.

Cybersecurity measures

b) Effective cybersecurity measures and policies should be implemented to minimise the risk exposure of designated wallets. Designated wallets should be designed and managed with a focus on privacy protection and in compliance with required confidentiality standards.

Principle 10: Valuation and realisation of value

1. General valuation criteria and realisation methods (such as judicial sale, private sale, auction) should be established for the valuation and the realisation of digital assets, and should be applied taking into consideration the characteristics of digital assets – volatility, lack of pricing mechanisms, and lack of recognised markets.

[22] See, for example, CEPEJ Guidelines 2009 under 36.

2. The choice of the realisation method to realise the value of digital assets as well as the time for such realisation by the selected method should be made by exercising the proper duty of care. Value maximisation, but also any risk of impact on market price, should be taken into consideration.

3. Where regulated or recognised markets for the trading of the (subclass of) digital assets subject to enforcement exist, these assets should be valued at the market price on the date of the enforcement action.

4. If no regulated or recognised market exists, and/or there are several possible markets, enforcement agents should take reasonable steps to maximise the realisation value, taking into consideration the circumstances, the characteristics of the subclass of digital assets, and valuation criteria for similar assets, where applicable.

Guidance to Principle 10

Realisation of the value

a) Taking into consideration the volatility of digital assets, States should consider the introduction into national law of a time limit within which digital assets should be realised.

The time limit should be reasonable to fulfil the enforcement goals and maximise the value. Other factors, such as the impact on market price, should be taken into account.

Valuation of the digital assets

b) As much as possible, existing provisions for the valuation of goods should be followed. The value of digital assets can be determined on the basis of an expert valuation or based on the market value in case a regulated or recognised market exists for such (class or subclass of) digital assets (eg crypto assets).

c) A valuation of the digital assets is not necessary where the parties to the enforcement procedure have determined the value of the digital assets by agreement.

The sale/transfer of digital assets

d) In conformity with the applicable realisation method, the digital assets:

d.1. should be transferred to the creditor at their request, as payment, under the supervision of the enforcement agent;

d.2. should be the subject of a forced judicial sale carried out by enforcement agents or through an exchange platform approved by the competent authority;

d.3. should be the subject of a judicial sale by public auction or any other judicial sale, in accordance with applicable law; or

d.4. should be the subject of a sale through a direct agreement.

In conformity with applicable law, any surplus generated by the transfer or sale of the digital assets is to be paid to the debtor.

If it transpires that auctions are unsuitable for digital assets due to higher associated costs and bidders prefer to acquire the digital assets at market price, as a rule, their sale through a direct agreement is the preferred method to maximise their value.

Professional liability

e) The risk of professional liability of enforcement agents should be covered by liability insurance, taking into consideration the average number and average value of cases as well as the complexity of enforcing against digital assets.

Annex: List of Sources

- Recommendation (16) 2003 of the Committee of Ministers to Member States on the Execution of Administrative and Judicial Decisions in the field of Administrative Law (referred as Rec 16(2003))
- Recommendation Rec (17) 2003 of the Committee of Ministers to Member States on Enforcement (referred as Rec 17(2003)
- Opinion No 13 (2010) of the Council of Europe, Consultative Council of European Judges on 'The role of judges in the enforcement of judicial decisions'
- CEPEJ Guidelines for a better implementation of the existing Council of Europe's Recommendation on Enforcement, European Commission on the efficiency of Justice (CEPEJ), (referred as: CEPEJ (2009))
- The Good practice guide on enforcement of judicial decisions adopted by CEPEJ in 2015
- UIHJ Global Code of Enforcement, 2024
- UNIDROIT Principles on Digital Assets and Private Law
- UNIDROIT Best Practices on Effective Enforcement

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9505495-5-3