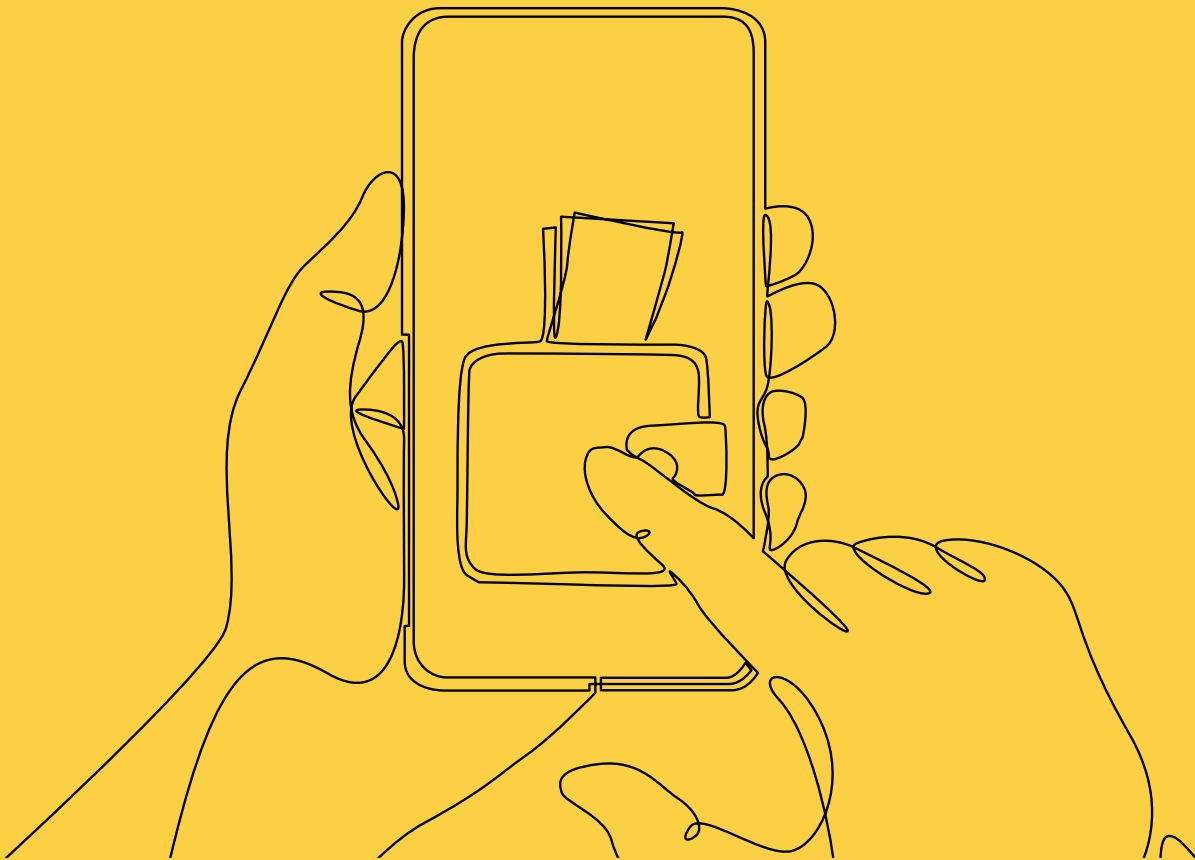


Model Rules on Succession and Access to Digital Remains

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.

President: Teresa Rodríguez de las Heras Ballell

First Vice-President: Sir Geoffrey Vos

Second Vice-President: Pietro Sirena

Treasurer: Anne Birgitte Gammeljord

Speaker of the Senate: Reinhard Zimmermann

Secretary-General: Vanessa Wilcox

Scientific Director: Christiane Wendehorst

European Law Institute

Schottenring 16/ 175

1010 Vienna

Austria

Tel: + 43 1 4277 22101

E-mail: secretariat@europeanlawinstitute.eu

Website: www.europeanlawinstitute.eu

Approved by the ELI Council on 24 June 2026 and by the ELI Membership on 16 July 2026.

Published on 28 August 2026.

ISBN: 978-3-9505990-5-3

© European Law Institute 2026

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



universität
wien

Table of Contents

Acknowledgements	6
Executive Summary	9
Introduction	11
Black Letter Rules	15
Chapter 1 Scope and Definitions	15
Chapter 2 Digital Succession	16
Chapter 3 Deletion of, and Access to, Personal Digital Remains	16
Chapter 4 Third-party Rights and Interests	18
Chapter 5 Applicable Law and Jurisdiction	19
Commentary	20
Chapter 1 Scope and Definitions	20
Chapter 2 Digital Succession	25
Chapter 3 Deletion of, and Access to, Personal Digital Remains	28
Chapter 4 Third-party Rights and Interests	33
Chapter 5 Applicable Law and Jurisdiction	35

Acknowledgements

Project Team

Reporters

Edina Harbinja (Associate Professor, UK)

Antoine Eigenmann (Lawyer and Professor, Switzerland)

Other Members of the Project Team

Philipp Ceesay (Professor, Germany)

Elwira Macierzyńska-Franaszczyk (Professor, Poland)

Francesco Paolo Patti (Professor, Italy)

Tamás Sajben (Notary, Hungary)

Project Assistant

Tal Morse (Lecturer, Israel)

Advisory Committee

Assessors

Teresa Rodríguez de las Heras Ballell (Professor, Spain)

François Trémosa (Notary, France)

Xandra Kramer (Professor, The Netherlands)

Other Members of the Advisory Committee

Sergio Cámara Lapuente (Professor, Spain)

Gregor Christandl (Professor, Austria)

Katell Drouet-Bassou (Lawyer, Switzerland)

Ben Furlong (Managing Director, UK)

Martin Hanzl (Lawyer, Austria)

Vasileios Karagiannopoulos (Associate Professor, UK)

Stacey Pitsillides (Associate Professor, UK)

Eleonora Rosati (Professor, Sweden)

Sjef van Erp (Emeritus Professor, The Netherlands)

Francesco Armando Schurr (Professor, Austria)

Members Consultative Committee

Peter Adler (Mediator, Austria)

Pinar Çağlayan Aksoy (Assistant Professor, Turkey)

Pilar Álvarez Olalla (Professor, Spain)

Arvind Babajee (Corporate Jurist / Chartered Management Accountant, Mauritius)

Teresa Bielska-Sobkowicz (Judge, Poland)

Mircea Dan Bob-Bocşan (Professor, Romania)

Ádám Boóc (Professor, Hungary)

Margareta Brattström (Supreme Court Justice, Sweden)

Robert Bray (†)

Suzanne Brown Walsh (Lawyer, USA)

Rebeca Carpi (Associate Professor, Spain)

Octavian Cazac (Associate Professor, Moldova)

Ana María Cediell Serra (Assistant Lecturer, Spain)

Tomasz Chmielewski (Lawyer, Poland)

Valeria Confortini (Professor, Italy)

Letizia Coppo (Associate Professor, France)

Andrea Dalmartello (Associate Professor, Italy)

Riccardo de Caria (Associate Professor, Italy)

Anabela Susana de Sousa Gonçalves (Associate Professor, Portugal)
 Mustafa Ebaid (Legal Researcher, Palestine)
 José Pau Echave (Lecturer, Spain)
 María Paz García Rubio (Professor, Spain)
 Rosa M. García-Teruel (Assistant Professor, Spain)
 Hristina Georgieva (Lawyer, Bulgaria)
 Marco Giacalone (Research Professor, Belgium)
 Nuria Ginés Castellet (Associate Professor, Spain)
 Isabel Victoria González Pacanowska (Professor, Spain)
 Elise Goossens (Assistant Professor, Belgium)
 Susanne Lilian Gössl (Professor, Germany)
 Mateusz Grochowski (Associate Professor, USA)
 Biset Sena Güneş (Senior Research Fellow, Germany)
 Emilia Hörnell (Lawyer, Sweden)
 Guillem Izquierdo Grau (Associate Professor, Spain)
 Monika Jagielska (University Professor, Poland)
 Melanija Jančić Mihić (Associate Professor, Serbia)
 Francisco Javier Jiménez Muñoz (Professor, Spain)
 Sara Johnson (Lawyer, Canada)
 Monika Jurčová (Professor, Slovakia)
 Kadir Berk Kapanci (Professor, Turkey)
 Aileen Keogan (Lawyer, Ireland)
 Alexander Keys (Lawyer, Belgium)
 Ben Köhler (Junior Professor, Germany)
 Pavel Koukal (Associate Professor, Czech Republic)
 Sophio Kurtauli (Lawyer, Georgia)
 Gökçe Kurtulan Güner (Assistant Professor, Turkey)
 Simon Laimer (University Professor, Austria)
 Ilse Marije Lambers (PhD Researcher, Netherlands)
 Antonio Legerén Molina (Associate Professor, Spain)
 John Linarelli (Professor, USA)
 Francesco Longobucco (Professor, Italy)
 José Luis Fernández Lozano (Notary, Spain)
 Timothy Lyons KC (Barrister, UK)
 Alisdair MacPherson (Senior Lecturer, UK)
 Geo Magri (Associate Professor, Italy)
 Carlos Marinho (Judge, Portugal)
 Claudia Elena Marinică (Lecturer, Romania)
 Giuseppe Marino (Associate Professor, Italy)
 Cristina Mariottini (Senior Lecturer, Luxembourg)
 Luz María Martínez Velencoso (Professor, Spain)
 Marco Martino (Professor, Italy)
 Maarten R. Meijer (Former Civil-Law Notary, Netherlands)
 Attila Menyhárd (Professor, Hungary)
 Dorota Miler (University Professor, Poland)
 Iain Mitchell KC (Barrister, UK)
 Carmen Muñoz García (Associate Professor, Spain)
 Daniele Muritano (Notary, Italy)
 Margot Musson (Lecturer, France)
 Kristin Nemeth (Assistant Professor, Austria)
 Niccolò Travia (Lawyer, Italy)

Yuko Nishitani (Professor, Japan)
Bahar Öcal Apaydın (Associate Professor, Turkey)
Ioana Olaru (Notary, Romania)
Konrad Osajda (Professor, Poland)
Marlena Pecyna (University Professor, Poland)
Luca Ettore Perriello (Associate Professor, Italy)
Thomas Pfeiffer (Professor, Germany)
Alain Pilette (EU Official, Belgium)
Katarzyna Południak-Gierz (Assistant Professor, Poland)
Rui Miguel Prista Patrício Cascão (Associate Professor, Portugal)
Karin Raková (Assistant Professor, Slovakia)
Caroline Rapatz (Professor, Germany)
Frederick Rieländer (Professor, Germany)
Sara Rodríguez Marín (Lawyer, Spain)
Albert Ruda (Associate Professor, Spain)
Carlo Rusconi (Researcher, Italy)
Leigh Sagar (Barrister, UK)
Pablo Salvador-Coderch (Emeritus Professor, Spain)
Alina Raluca Sarchisian (Lawyer, Romania)
Vyara Savova (Lawyer, Bulgaria)
Christian Schall (Notary, Germany)
Jan Peter Schmidt (Senior Research Fellow, Germany)
Stacie Strong (Professor, USA)
Emir Sudžuka (Notary, Bosnia and Herzegovina)
Ferenc Szilágyi (Associate Professor, Hungary)
Paula Távora Vítor (Assistant Professor, Portugal)
Rute Teixeira Pedro (Associate Professor, Portugal)
Eric Tjong Tjin Tai (Professor, Netherlands)
Camelia Toader (Professor, Romania)
Stefano Troiano (Professor, Italy)
Colin Tyre (Judge, UK)
Antoni Vaquer Aloy (Professor, Spain)
Gabriela Varia (Lecturer, Romania)
Vanessa Villanueva Collao (Senior Research Fellow, Australia)
Asim Vokshi (Judge, Albania)
Denise Wiedemann (Professor, Germany)
Eleni Zervogianni (Associate Professor, Greece)
Irina Zlătescu (Professor, Romania)

Observers

European Commission (represented by Maria Vilar Badia)
Digital Legacy Association (represented by James Norris)
Society of Trust and Estate Practitioners (STEP) (represented by Jack Burroughs)
Uniform Law Commission (ULC) (represented by Suzanne Brown Walsh)
Uniform Law Conference of Canada (ULCC) (represented by Donna L Molzan, KC)
Council of the Notariats of the European Union (CNUE) (represented by Marianne Sevindik and Philip Bender)

ELI Project Officer

Tomasz Dudek (Senior Project Officer, Austria)

Executive Summary

These Model Rules set out a framework for succession to digital assets and access to personal digital remains after death. They address the growing practical and legal difficulties that arise when a person dies leaving online accounts, digital assets, cloud-stored materials, personal data, communications, and digital or AI-generated representations. The Model Rules aim to provide legal certainty while respecting the privacy and dignity of the deceased, the rights and interests of heirs and other beneficiaries, the rights of living third parties, and the obligations of service providers.

The Model Rules are built around the concept of 'digital remains'. This umbrella concept includes both digital assets and personal digital remains. A digital asset is a digital remain capable of control, enjoyment or use, and capable of transfer, irrespective of whether the relevant right is characterised as proprietary, contractual or otherwise. Personal digital remains are digital remains that, by their nature or function, reflect, express or are intrinsically linked to the deceased's personality, identity or private life. They include the deceased's personal data and digital representations capable of evoking, simulating, re-performing or reconstructing aspects of the deceased's personality, likeness, voice, presence or behaviour, including through automated or generative systems.

A central feature of the Model Rules is the distinction between succession and access. Digital assets are governed by succession law. Personal digital remains are governed by a separate access regime. Where a single digital remain contains both a digital asset and personal digital remains, the access regime applies first to the personal elements before the asset is dealt with under succession law, unless the personal element is merely ancillary to the asset. This approach prevents personality-linked material from being treated as ordinary property while preserving the transferability of economic digital assets.

The Model Rules provide that digital succession is governed by the rules applicable to succession to movable property, with such modifications as are necessary to reflect the nature of digital assets. Service providers must enable the orderly transfer of digital assets by providing appropriate mechanisms, clear and accessible tools or platform rules, and adequate notice before discontinuing services so that estate representatives can export digital assets.

Terms and conditions that prevent or hinder the transfer of digital assets are invalid unless individually negotiated with the deceased, with the burden of proof placed on the service provider.

For personal digital remains, the Model Rules recognise the deceased's autonomy. The deceased may direct the deletion of all or some personal digital remains. If no such deletion direction applies, beneficiaries may exercise an access right. This right includes access, use, disclosure, preservation, rectification, obtaining a copy, transfer and deletion of the content of personal digital remains. It is time-limited: access and preservation rights expire ten years after death, and service providers may not charge fees for the exercise of those rights during that period.

The Model Rules also identify the beneficiaries of the access right. Priority is given to persons explicitly designated by the deceased. In the absence of such designation, access may be granted to intestate heirs, universal heirs or residuary beneficiaries, and executors or administrators of the estate. The State or an administrative unit is excluded where it would otherwise inherit on intestacy. The deceased may also exclude or limit access, provided the exclusion or limitation is specific and clearly identifies the personal digital remains concerned.

The deceased's directions may be made by testamentary disposition, through an online tool provided by a service provider, or by written statement to the service provider or person controlling the relevant medium. Where several directions conflict, the most recent direction prevails, provided that its date can be reasonably established. This mechanism is intended to respect autonomy while giving service providers and beneficiaries an operationally clear method for resolving inconsistent instructions.

The Model Rules further require service providers to preserve personal digital remains for five years after death, unless the deceased directed or consented to deletion, or beneficiaries validly request deletion or modification. After five years, service providers and others controlling the relevant medium may delete personal digital remains unless preservation has been requested by a beneficiary or a third party has notified a legitimate claim to access.

Because digital remains often contain information about persons other than the deceased, the Model Rules include safeguards for third parties. A third party with a legitimate interest, for example because of legal proceedings or contractual obligations, may request access to the content of digital remains. Conversely, a third party whose rights would be infringed by continued access or preservation may request deletion, exclusion or limitation of access. Any measure must be proportionate. Where heirs or beneficiaries fail to comply, and continued retention would seriously and disproportionately infringe third-party rights, a service provider may be required to restrict access or cease preservation, subject to written reasons and judicial review.

The Model Rules do not create autonomous private international law rules. They apply without prejudice to applicable EU or national rules on applicable law and jurisdiction, including in matters of digital succession and access to personal digital remains. For non-EU countries, they likewise apply without prejudice to applicable national private international law rules.

Overall, the Model Rules offer a structured and practical framework for post-mortem digital governance. They preserve succession to transferable digital assets, establish a distinct access regime for personality-linked digital remains, protect the deceased's autonomy and dignity, safeguard third-party rights, and impose workable obligations on service providers and others who control digital remains. Their purpose is to support coherent national and European approaches to digital succession and access, while avoiding reducing all digital remains to either property or personal data.

Introduction

1. The Digital Footprint

Digital remains are now part of everyday life. Most people leave behind a substantial digital footprint when they die: online accounts, cloud storage, emails and messages, social media profiles, subscriptions, digital wallets and crypto-assets, creative works, business tools, and, increasingly, new forms of digitally mediated identity, such as avatars or AI-enabled chatbots trained on personal data and the deceased's likeness (often described as 'deadbots' or 'ghostbots'). These materials may hold economic value, deep personal or sentimental value, or both. They also routinely contain personal data about the deceased and living third parties.

In these Model Rules, the term 'digital remains' is used as an umbrella concept encompassing all digital items, records and representations, whether stored in an online account operated by a service provider or on a physical device owned by the deceased. Importantly, the Rules explicitly exclude electronic records maintained by third parties for their own institutional purposes (such as hospital, banking, or public authority databases) where the deceased's only rights were those of a data subject under data protection law.

2. The Governance Gap

Death exposes a practical governance gap. When a person dies, families, executors, and service providers need workable answers to three questions: What remains exists? Who may access or inherit it? Under what privacy safeguards? At present, existing law does not provide a coherent pathway, leading to three distinct problems:

- **The succession problem:** Traditional succession law is designed to transmit mostly economic wealth, making it the natural mechanism for transferring commercial digital assets and property (although many national

systems do not yet explicitly recognise purely digital items as inheritable property). However, succession law is unsuited for governing personal data, private communications, and personality-linked materials, which cannot, and should not, be treated as inheritable property. Furthermore, even when a digital item is clearly an economic asset, it is frequently intertwined with vast amounts of personal data, which cannot be passed on, making succession unsuitable without a prior mechanism to access, filter, or remove that sensitive personal information.

- **The contract problem:** In the absence of clear legislation, service providers' Terms of Service act as the default law. Although a small number of providers offer services such as legacy contacts to help users make decisions regarding their digital content, these contracts routinely prohibit the transfer of, or access to, digital accounts upon death, allowing service providers to act as gatekeepers and undermining legitimate succession and access rights.
- **The cross-border problem:** Digital remains are frequently stored on foreign servers, under contracts governed by foreign laws. The absence of harmonised private international law rules for digital remains complicates cross-border estates, leaving heirs unable to enforce their rights abroad.

3. The Core Solution: A Two-Regime Approach

To resolve these issues, the Model Rules make a fundamental policy choice. They reject the false simplicity of either treating all digital files as 'inheritable property' or of treating all files as 'personal data'. Instead, the Rules establish two

distinct legal regimes based on the nature of the digital remains:

- **Regime 1: Digital Succession (for Digital Assets).** Digital assets are digital remains capable of control, enjoyment, or use and are transferable. They automatically fall under the ordinary law of succession, just like physical property.
- **Regime 2: The Access Right (for Personal Digital Remains).** Personal Digital Remains (PDRs) are items intrinsically linked to the deceased's personality, identity, or private life, including personal data and AI simulations of the deceased. Because they implicate dignity, autonomy and privacy, PDRs *do not* fall under the ordinary law of succession. Instead, they are subject to a structured, temporary, and safeguarded right of access granted to specific beneficiaries under these Rules.

In practice, however, digital life is heavily integrated. Many digital environments and records simultaneously contain both digital assets and personal digital remains, which the Model Rules address through a dedicated framework for 'mixed cases'.

4. Basic Classifications under the Rules

To illustrate this dividing line, the Rules apply a 'nature' test:

- **Pure Digital Assets (Succession):** Examples of such assets are, among others, a digital bank balance, a crypto-wallet, a monetised video channel, or a registered domain name. These are economic, controllable, transferable, and transfer directly to the heirs.
- **Pure Personal Digital Remains (Access Right):** Examples include a memorial chatbot designed to simulate the deceased or a private dating app profile. These are entirely personality-driven. They do not pass to the heirs as property. Beneficiaries may access or delete them in accordance with the deceased's wishes and the access rights under these

Rules, but they cannot 'inherit' the deceased's digital identity.

- **Personal Data and Digital Assets (Mixed Records):** It is highly common for a mixed case to have digital assets and embedded personal data. Unless personal data are ancillary (eg, a crypto-exchange account will contain the deceased's identification data, where the succession regime applies), personal data will trigger the access regime's safeguards (eg, emails containing private communications and copyrightable poems). The beneficiaries can address the personal data layer (eg, by deleting highly sensitive information) before the underlying economic asset is transferred to the heirs.
- **Basic Communications and Media (Access Right / Mixed):** Non-business personal emails and social media profiles are predominantly personal and fall under the access right. Photographs that include identified or identifiable individuals are generally personal, and the right of access under these Rules applies. However, if a photograph reaches the threshold of originality to qualify for commercial copyright (and most will), that specific intellectual property right operates as a digital asset under succession law, even if the image contains personal data. Photographs may also be considered digital assets in their own right, in which case the succession regime applies.

5. Mixed Cases and the Sequencing Rule

One of the central difficulties is that digital life is heavily integrated. 'Mixed cases' occur when digital assets and PDRs are bundled together. This can happen at an *environment level* (eg, an iCloud account containing valuable business Intellectual Property (IP), private communications, and intimate family photos) or at a *record level* (eg, a single draft manuscript that holds copyright value but contains sensitive medical data).

To resolve mixed cases, the Rules apply a strict sequence:

1. Assess the environment/record to identify personal material. This would normally be done by personal representatives/executors where they exist or service providers.
2. Give effect to the deceased's directives (eg, an instruction to delete certain files).
3. Apply the access safeguards to the personal layer (allowing beneficiaries to redact, extract, or delete sensitive personal data).
4. **Only then** complete the transfer of the remaining inheritable digital asset to the successors.

If the personal data is merely ancillary (eg, the deceased's name attached to a crypto-wallet), the asset passes under succession without triggering the full access regime.

6. The Role of Service Providers and the Expiration of Access

The deceased's wishes are paramount. Individuals may direct deletion by the service provider or designate a specific person to exercise the access right. Where no directives exist, service providers are legally required to preserve personal digital remains for five years following death to ensure beneficiaries have sufficient time to secure the estate. However, to reflect the nature of post-mortem privacy across European legal systems, the right of access expires ten years after death.

7. Third-Party Rights

Because digital remains (like emails and shared documents) frequently contain the personal data of living third parties, the Rules provide a framework aligned with the General Data Protection Regulation (GDPR). Third parties who demonstrate a legitimate interest may request access to data. In particular, third parties whose privacy would be infringed may also request that beneficiaries delete or limit access to specific remains. If a beneficiary unjustifiably refuses,

and the retention would seriously infringe the third party's rights, the service provider may be compelled to intervene.

8. Cross-Border Enforcement and Systemic Integration

Cross-border enforcement and jurisdiction are critical for the effectiveness of this framework. Because digital remains are frequently stored on foreign servers under contracts governed by foreign law, the Model Rules deliberately align applicable law and jurisdiction with the existing framework of European private international law. Rather than creating autonomous conflict-of-laws rules or overriding mandatory provisions, the Rules adopt a conservative approach. Accordingly, they apply without prejudice to EU or national private international law instruments.

Digital succession (determining who inherits the asset) falls within the scope of Regulation (EU) No 650/2012 (the Succession Regulation). The contractual relationships between the deceased and service providers (which govern the terms of access to digital assets and personal digital remains) are governed, as regards applicable law and jurisdiction, by Regulation (EC) No 593/2008 (Rome I) and Regulation (EU) No 1215/2012 (Brussels Ibis).

Under this approach, the law applicable to the contract, including any chosen foreign law or jurisdiction clause stipulated by the usual platform terms, remains effective. Consequently, disputes concerning digital assets or access rights may be subject to foreign law and foreign courts where validly agreed. This preserves systemic coherence with the current EU private international law framework and avoids fragmentation, though it relies significantly on existing consumer protection safeguards (such as Article 6 of Rome I and Article 17 of Brussels Ibis) to protect heirs and beneficiaries against potentially abusive non-local platform terms. The Model Rules, therefore, operate within, rather than displace, the existing European conflicts architecture.

9. Comprehensive Illustration

D dies in Spain, leaving: (a) a Revolut account; (b) an iCloud photo library; (c) an email account containing business and personal emails; (d) a draft manuscript in the cloud; and (e) a custom AI deadbot. The US-based cloud provider's terms mandate California law.

- **The Revolut balance** is a digital asset. It transfers under Spanish succession law.
- **The iCloud photo library and personal emails** are PDRs. Beneficiaries are granted access to download family photos for private purposes but cannot 'take over' the account and act as the deceased. Digital photos may also be subject to succession as digital assets and/or copyright and would pass to a successor (subject to removal of personal data). Emails that include content that satisfies copyright requirements (originality, in particular) would pass on to a successor, but after the access regime is applied to personal data usually included therein. Third-party privacy in communications is protected under the GDPR.
- **The business correspondence** may be accessed specifically to administer the estate or conduct the dispute and pass to whoever succeeds to the business, applying data minimisation and other relevant GDPR principles.
- **The draft manuscript** is a mixed case. The beneficiaries may access it to redact or address the sensitive personal references (PDR layer) before the manuscript's copyright (asset layer) is transferred to the heirs for publication.
- **The AI deadbot** is strictly a PDR. It does not pass under succession. Beneficiaries may delete or preserve it under the Model Rules' access regime as long as they do not impersonate the deceased, but do not acquire property rights to commercially exploit the deceased's likeness.
- **Cross-Border Enforcement:** Because the Model Rules integrate with existing EU private international law, Spanish law (as the *lex successionis* under Regulation 650/2012) determines who inherits the Revolut balance

and any transferable digital assets. However, the contractual relationship with the US-based cloud provider remains governed by California law and subject to California courts to the extent that such clauses are effective under Rome I and Brussels Ibis. As a result, while heirs succeed to inheritable assets under Spanish law, disputes concerning access to the iCloud library, email account, or manuscript could be subject to foreign law and jurisdiction clauses contained in the platform's standard terms, subject only to the consumer protection safeguards available under those Regulations. The Model Rules, therefore, ensure unity of succession while accepting that contractual enforcement may remain transnational and platform-mediated.

10. Aim and Intended Uptake

These Model Rules are drafted for adoption in national law and, where appropriate, for EU-level development. Their purpose is to reduce uncertainty, prevent avoidable distress and conflict, and provide a workable framework for service providers, legal professionals, and citizens.

Black Letter Rules

Chapter 1

Scope and Definitions

Article 1 *Purpose and scope*

1. These Model Rules govern rights and obligations in respect of digital remains following a person's death, having regard to:
 - a. the privacy and dignity of the deceased; and
 - b. the rights and interests of heirs, other beneficiaries, and third parties.
2. The Model Rules govern:
 - a. succession to digital assets;
 - b. access to personal digital remains; and
 - c. the obligations and responsibilities of service providers and others having control of digital remains.
3. These Model Rules do not apply to electronically stored records maintained by third parties for their own purposes, where the deceased's solely held rights were those of a data subject under data protection law.

Article 2 *Definitions*

1. '*Digital remain*' means any item in digital form to which the deceased had an entitlement, or any record or representation in digital form that comprises, records or represents a

right or interest held by the deceased during their lifetime, including where it is a record or representation of a real-world, tradeable asset, and regardless of whether or not it is held directly or through an intermediary, together with any information associated therewith.

Digital remains include digital assets, as defined in paragraph 2, and personal digital remains, as defined in paragraph 3. A single digital remain may contain both digital assets and personal digital remains (a 'mixed case').

2. '*Digital asset*' means any digital remain that fulfils the following criteria:
 - a. it is capable of being subject to a right of control, enjoyment or use, regardless of whether such rights are legally characterised as being of a proprietary, obligational or other nature; and
 - b. it is capable of being transferred from one party to another, including by way of voluntary disposition.

A digital remain may qualify as a digital asset notwithstanding that it contains, or is inextricably linked to, personal data.

3. '*Personal digital remain*' means a digital remain which, by its nature or function, reflects, expresses, or is intrinsically linked to the deceased's personality, identity or private life, and includes, in particular:
 - a. the deceased's personal data; and
 - b. digital representations designed or reasonably capable of evoking, simulating, re-performing, or materially reconstructing aspects of the deceased's personality, likeness, voice, presence or behaviour, including through automated and generative systems.

4. **'Personal data'** has the same meaning as conferred by Article 4(1) of Regulation (EU) 2016/679, and, for the purposes of these Model Rules, also includes the deceased's personal data.
5. **'Digital succession'** means the transfer of digital assets on death, including the inheritance, distribution, and administration of those assets.
6. **'Access right'** means a right to access, use, disclose, require the preservation of, rectify, obtain a copy of (including by download/export), transfer, and delete the content of the personal digital remains.
7. **'Beneficiaries'** means the persons listed in Article 7.

Article 3 Mixed cases

1. Where a single digital remain contains both digital assets and personal digital remains, then, subject to paragraph 2, the access regime in Chapter 3 must be applied to the personal digital remains before the digital asset is dealt with under succession law.
2. The access regime under Chapter 3 shall not apply where the personal element is merely ancillary to a digital asset. In this case, Chapter 2 applies.

Chapter 2

Digital Succession

Article 4 Digital succession

1. Digital succession shall be governed by the rules that the law of succession prescribes for

succession to movable property, with such modifications as may be necessary to give effect to the nature of the digital assets.

2. Service providers must ensure the orderly transfer of digital assets by:
 - a. providing mechanisms to enable such transfer in accordance with applicable succession laws;
 - b. providing clear, accessible, and enforceable tools or platform rules; and
 - c. issuing adequate prior notice and allowing representatives of the estate to export digital assets in an appropriate format before discontinuing a service.
3. Any term in a service provider's terms and conditions that purports to prevent or hinder the transfer of digital assets in accordance with this Article will be invalid unless it was individually negotiated with the deceased. The service provider shall bear the burden of proving that any such clause was individually negotiated with the user.
4. Where no service provider is involved, the person who controls the medium on which the digital asset is recorded must enable the digital asset to be transferred.

Chapter 3

Deletion of, and Access to, Personal Digital Remains

Article 5 Deletion

The deceased may direct that all or any of their personal digital remains held by a service provider with whom the deceased had an account, or by the person who controls the medium on which the personal digital remains are recorded, shall be deleted.

Article 6

Access right

1. Personal digital remains that have not been deleted in accordance with the directions of the deceased are subject to a right of access by the beneficiaries listed in Article 7.
 2. The beneficiaries may exercise the right of access against the service provider with whom the deceased had an account, or where no service provider is involved, against the person who controls the medium on which the personal digital remains are recorded.
 3. Any right of access to personal digital remains, or right to require their continued preservation, shall expire after ten years from the date of the deceased's death.
 4. During the period referred to in paragraph 3, service providers and persons who control the medium on which the personal digital remains are recorded shall not charge a fee for the exercise of the access right or the right to require preservation under this Chapter.
 5. Any term in a service provider's terms and conditions that purports to prevent or hinder access or compliance with directions given in accordance with this Chapter will be invalid unless the term was individually negotiated with the deceased. The service provider shall bear the burden of proving that any such term was individually negotiated with the user.
- b. where the deceased has died intestate, the heirs under the applicable laws of succession (provided that the heir is not the State or an administrative unit);
 - c. where the deceased has left a valid will, the universal heirs or residuary beneficiaries of the estate; and
 - d. executors or administrators of the estate.
2. Where the deceased has designated a person to exercise the access right in respect of all or specified personal digital remains, the beneficiaries listed in paragraph 1(b)–(d) shall not be entitled to exercise the access right in respect of those personal digital remains, except insofar as access is necessary for the settlement of the deceased's estate.
 3. The deceased may exclude or limit access to personal digital remains by the beneficiaries listed in paragraph 1.
 4. Exclusions or limitations must:
 - a. be specific in scope; and
 - b. clearly identify the personal digital remains affected.
 5. Personal digital remains shall not be modified or deleted under this Article, and access to them shall not be excluded or limited under this Article or Article 8, insofar as access to them by the representatives of the deceased's estate is necessary for the settlement of the deceased's estate.

Article 7

Beneficiaries of the access right

1. Access to personal digital remains is granted to the following beneficiaries:
 - a. persons explicitly designated by the deceased;
6. Personal digital remains shall not be modified or deleted under this Article, and access to them shall not be excluded or limited under this Article or Article 8, to the extent that such modification or deletion or exclusion or limitation of access would be incompatible with the rights of a third party.
 7. Where there are multiple beneficiaries under this Article, and the deceased has not given any other directions, none of the

beneficiaries is entitled to delete or modify any personal digital remains unilaterally. If a beneficiary unreasonably refuses to consent to the deletion or modification of personal digital remains, the other beneficiaries may bring the matter before a court to obtain a decision in lieu of unanimous consent.

Article 8

Directives, methods and priority

1. The deceased's directives under Articles 5, 6 and 7 (deletion, designation, exclusion or limitation) may be issued through:
 - a. testamentary dispositions;
 - b. an online tool provided by the service provider that also records the date of the directive; and
 - c. a written statement directed to the service provider or the person who controls the medium on which the personal digital remain is recorded.
2. Where the deceased has given more than one designation of a beneficiary and/or more than one directive, and the designations and/or directives are not consistent with each other, the most recent designation or directive prevails, provided that the date of its making can be reasonably established. Nothing in this paragraph affects the formal validity of a testamentary disposition under the applicable succession law.
3. Service providers must act in reliance on the latest designation or directive made via the online tool unless they are informed of a later designation or directive within six months after death.

Article 9

Preservation and exceptions

1. During the first five years following death, a service provider must preserve personal digital remains to enable access under this Chapter unless:
 - a. the deceased gave directions for, or explicit prior consent to, deletion, either by an individually negotiated term or by means described in Article 8(1); or
 - b. the beneficiaries submit a request for modification or deletion of the personal digital remains in accordance with Article 7 paragraph 7.
2. After five years, service providers, and other persons who control the medium on which the personal digital remains are recorded, may delete personal digital remains unless they have received a request for their continued preservation by a beneficiary under Article 7, or they have been given notice of a legitimate claim to access the content of the remains by a third party in accordance with Article 10.

Chapter 4

Third-party Rights and Interests

Article 10

Third-party rights and interests

1. A third party who demonstrates a legitimate interest (eg because of ongoing legal proceedings or contractual obligations) shall have a right to request access to the content of digital remains from a successor to the digital asset under Chapter 2 or a beneficiary under Chapter 3.

2. A third party who demonstrates that continued access to, or preservation of, digital remains would infringe their rights shall have a right to request deletion, exclusion, or limitation of access to digital remains from a successor to the digital asset under Chapter 2 or a beneficiary under Chapter 3. The measure requested shall be proportionate to the risk that continued access to, or preservation of, the digital remains would pose to third-party rights.
3. Where an heir or a beneficiary fails to comply with a request under paragraph 2, and where continued retention of the digital remains would seriously and disproportionately infringe third-party rights, a service provider shall, upon request of the third party, exclude or limit access or cease preservation provided that reasons are given in writing and, where contested, the measure is subject to judicial review.
4. These rules apply without prejudice to any rights the third party may have under data protection law or any other law.

Chapter 5

Applicable Law and Jurisdiction

| Article 11

1. These Model Rules apply without prejudice to applicable EU or national private international law rules, in particular those concerning applicable law and jurisdiction in matters of digital succession or access rights to personal digital remains.
2. *For non-EU countries:* These Model Rules apply without prejudice to applicable national private international law rules, in particular those concerning applicable law and jurisdiction in matters of digital succession or access rights to personal digital remains.

Commentary

Chapter 1

Scope and Definitions

Article 1 *Purpose and scope*

1. These Model Rules govern rights and obligations in respect of digital remains following a person's death, having regard to:
 - a. the privacy and dignity of the deceased; and
 - b. the rights and interests of heirs, other beneficiaries, and third parties.
2. The Model Rules govern:
 - a. succession to digital assets;
 - b. access to personal digital remains; and
 - c. the obligations and responsibilities of service providers and others having control of digital remains.
3. These Model Rules do not apply to electronically stored records maintained by third parties for their own purposes, where the deceased's solely held rights were those of a data subject under data protection law.

Article 2 *Definitions*

1. '*Digital remain*' means any item in digital form to which the deceased had an entitlement,

or any record or representation in digital form that comprises, records or represents a right or interest held by the deceased during their lifetime, including where it is a record or representation of a real-world, tradeable asset, and regardless of whether or not it is held directly or through an intermediary, together with any information associated therewith.

Digital remains include digital assets, as defined in paragraph 2, and personal digital remains, as defined in paragraph 3. A single digital remain may contain both digital assets and personal digital remains (a 'mixed case').

2. '*Digital asset*' means any digital remain that fulfils the following criteria:
 - a. it is capable of being subject to a right of control, enjoyment or use, regardless of whether such rights are legally characterised as being of a proprietary, obligational or other nature; and
 - b. it is capable of being transferred from one party to another, including by way of voluntary disposition.

A digital remain may qualify as a digital asset notwithstanding that it contains, or is inextricably linked to, personal data.

3. '*Personal digital remain*' means a digital remain which, by its nature or function, reflects, expresses, or is intrinsically linked to the deceased's personality, identity or private life, and includes, in particular:
 - a. the deceased's personal data; and
 - b. digital representations designed or reasonably capable of evoking, simulating, re-performing, or materially reconstructing aspects of the deceased's

personality, likeness, voice, presence or behaviour, including through automated and generative systems.

4. **'Personal data'** has the same meaning as conferred by Article 4(1) of Regulation (EU) 2016/679, and, for the purposes of these Model Rules, also includes the deceased's personal data.
5. **'Digital succession'** means the transfer of digital assets on death, including the inheritance, distribution, and administration of those assets.
6. **'Access right'** means a right to access, use, disclose, require the preservation of, rectify, obtain a copy of (including by download/export), transfer, and delete the content of the personal digital remains.
7. **'Beneficiaries'** means the persons listed in Article 7.

Article 3 Mixed cases

1. Where a single digital remain contains both digital assets and personal digital remains, then, subject to paragraph 2, the access regime in Chapter 3 must be applied to the personal digital remains before the digital asset is dealt with under succession law.
2. The access regime under Chapter 3 shall not apply where the personal element is merely ancillary to a digital asset. In this case, Chapter 2 applies.

1. Scope and Design of the Model Rules (Article 1)

Articles 1–3 establish the conceptual architecture of the Model Rules. They respond to a recurring practical difficulty: when a person dies, it is often unclear what forms part of the estate (transferable under succession law), what constitutes intrinsically personal material (requiring special privacy safeguards), and how to handle digital environments where both coexist.

Article 1(1) makes explicit that the Rules are not merely succession provisions. They are structured to balance three core interests: the privacy and dignity of the deceased; the rights and interests of heirs, third parties, and beneficiaries (defined in Article 2 as the specific persons granted access rights under Chapter 3); and the obligations of service providers.

Importantly, Article 1(3) sets a strict boundary. It establishes that where a third party (eg, a hospital, public body, or bank) maintains electronic records for its own purposes, and the deceased's *only* rights were those of a data subject under the GDPR¹, the Model Rules do not apply. This ensures that the Rules focus strictly on the deceased's own digital estate and do not inadvertently grant heirs backdoor access to institutional databases.

2. 'Digital Remains' as the Umbrella Concept (Article 2(1))

Article 2(1) defines 'digital remains' as the overarching, technology-neutral category. It refers to any item or record in digital form to which the deceased had an entitlement, or which represents a right or interest held by the deceased.

The Model Rules recognise that what is colloquially called an 'account' is set up by a contract between the service provider and the deceased. The specific rights and assets recorded *inside* that account fall under the

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, possibly amended in the future, see the Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) [SWD(2025) 836 final], 21 November 2025.

umbrella of digital remains. The Rules require succession law to recognise these rights even if they are exclusively recorded or represented digitally. The definition encompasses both patrimonial (economic) interests and non-patrimonial (personality/privacy) interests, setting the stage for the two-regime classification.

3. The Two-Regime Structure (Article 2(2) & 2(3))

The Model Rules do not divide the digital world into two physical types of files; rather, they subject digital remains to **two distinct legal regimes**:

- **Regime 1: Digital Assets and Succession Law (Article 2(2)).** Digital assets are defined by their capacity for control, use, and transferability (akin to other definitions adopted by the European Law Institute (ELI), such as the ELI Principles on the Use of Digital Assets as Security).² While it is technically true that personal data or the deceased's chatbots *could* be controlled and transferred, the Model Rules make a strict normative choice. Applying property and succession law by default to one's 'informational body' or private communications would undermine human dignity.³ Therefore, personal digital remains, including chatbots of the deceased, are expressly excluded from the definition of a digital asset.⁴
- **Regime 2: Personal Digital Remains and the Access Right (Article 2(3)).** PDRs encompass any remains intrinsically linked by nature or function to the deceased's personality, identity, or private life.

This explicitly includes personal data (bridging the gap left by Recital 27 of the GDPR) and generative AI representations (eg, chatbots or deepfakes simulating the deceased).⁵ Because these items implicate dignity and privacy,⁶ they do not fall under succession law; they are governed strictly by the Chapter 3 access regime.

This deliberate legal separation ensures that highly personal items and personal data are not automatically inherited as property, while ensuring economic assets flow smoothly to successors.

4. Mixed Cases, Sequencing, and Intellectual Property (Article 3)

Because digital life is heavily integrated, Article 3 addresses 'mixed cases'. Mixing can occur at the **environment level** (an account holding both a crypto-wallet and private messages) or at the **record level** (a single file containing both economic and personal elements).

A common example of record-level mixing is a photograph. If a photograph meets the national originality threshold for copyright protection, that economic intellectual property right is a digital asset capable of succession. It could also satisfy the criteria for a digital asset under the Rules and some national laws. However, if the photograph depicts an identifiable living person, it may also reveal elements/information intrinsically linked to the deceased's personality and/or private life.

² ELI Principles on the Use of Digital Assets as Security; ELI Principles and Guidance for Enforcement Against Digital Assets; slightly different definitions are offered in ELI Principles and Guidance for Enforcement Against Digital Assets, B.1 and UNIDROIT Digital Assets and Private Law Principle 2(2), 2023.

³ Article 1 Charter of Fundamental Rights of the European Union; EU, European Declaration on Digital Rights and Principles for the Digital Decade, 15 December 2022, where digital legacy has been recognised as an important right; informational body is a concept developed by Floridi, see Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

⁴ The team also considered definitions from the following instruments: The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA 2015), Section 870 (h); Oregon State Bar Legislative Proposal to amend, among other provisions, OR. REV. STAT. 111.005 (2013); Uniform Law Conference of Canada, Uniform access to digital assets by fiduciaries act (2016), Article 1; UNIDROIT Digital Assets and Private Law Principle 2(2), 2023.

⁵ Edina Harbinja, Lilian Edwards & Marisa McVey, Governing ghostbots, 48 Computer Law & Security Review 105791 (2023); Edina Harbinja, Governing Digital Immortality: Artificial Intelligence, Deadbots and the Law (Edward Elgar, 2026, forthcoming).

⁶ See Edina Harbinja, Digital Death, Digital Assets and Post-mortem Privacy: Theory, Technology and the Law (2022); Michael Birnhack & Tal Morse, Digital remains: property or privacy?, International Journal of Law and Information Technology eaac019 (2022); J. C. Buitelaar, Post-mortem privacy and informational self-determination, 19 Ethics and Information Technology 129 (2017); Tina Davey, Until Death Do Us Part: Post-mortem Privacy Rights for the Ante-mortem Person, 2020; Gianclaudio Malgieri, R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions, in Data Protection and Privacy: The Internet of Bodies 143 (Ronald Leenes et al. eds., 2018); David Erdos, Dead ringers? Legal persons and the deceased in European data protection law, 40 Computer Law & Security Review 105495 (2021).

Article 3(1) resolves this through an “access-first” sequencing rule. Beneficiaries must apply the access regime first, addressing the privacy and data protection rights of the deceased protected under these Rules and living third parties protected under the GDPR (eg, by deleting or modifying it), *before* the heirs can commercially exploit the copyright under succession law.

Article 3(2) introduces the ‘ancillary’ test as a mechanism of proportionality. If personal data is merely incidental to the asset (eg, the deceased’s email address used solely as a login ID for a crypto-exchange), the full access-first procedure is bypassed, and Chapter 2 succession applies directly.

5. Illustrative Examples

- **Example 1 — Crypto wallet in cloud storage:** A cloud account contains private keys to a crypto wallet and minimal associated identifiers. *Application:* The personal data is merely ancillary. The item satisfies Article 2(2); succession law governs.
- **Example 2 — Social media account with copyrightable photos and private messages:** The account contains photos (some meeting copyright thresholds, possibly also constituting digital assets under the Rules) and intimate personal communications. *Application:* This involves both a mixed environment and mixed records. Access-first

sequencing applies. Personal communications are handled under the access regime. For the photos, privacy safeguards for depicted individuals are applied *before* any copyright interests are transferred to the heirs of photos as digital assets.

- **Example 3 — Generative AI Chatbot:** A deceased leaves behind a custom-trained AI chatbot simulating their personality. *Application:* Under Article 2(3)(b), this is explicitly classified as a Personal Digital Remain. It cannot be inherited as a digital asset. It is governed entirely by the access right (including deletion), protecting the deceased’s digital dignity from unauthorised exploitation by successors. If not deleted, it will be subject to the same access rights as other personal digital remains.

6. Comparative Law, Personality Rights, and the Model Rules

Because European jurisdictions vary widely in their treatment of post-mortem privacy and personality rights, the Model Rules do not rely on a single national doctrine. Instead, they use ‘personal data’ as an administrable anchor for the access regime, while expressly allowing national personality rights to apply where recognised.

The table below outlines how the Model Rules interact with, and differ from, existing national approaches:

Concept/Jurisdiction	Legal Basis	Post-mortem Status	How the Model Rules’ Outcome Differs/Interacts
Germany	Constitutional and civil law, including personality rights ⁷ and universal succession	Universal succession applies to social media accounts (BGH <i>Facebook</i> case ⁸). Commercial aspects of personality rights may fall under succession.	Differs strictly: The Model Rules reject universal succession for PDRs. A purely personal account or AI chatbot cannot be inherited as property.

⁷ Case of the Advertisements of Dietrich (*Marlene*) (BGHZ 143, 214)

⁸ *Facebook* inheritance case (BGH III ZR 183/17)

Concept/Jurisdiction	Legal Basis	Post-mortem Status	How the Model Rules' Outcome Differs/Interacts
France/Spain/Italy	Civil Codes/specific data protection statutes ⁹	Relatives/heirs granted statutory rights to access, rectify, or delete the deceased's personal data.	Expands and clarifies: While aligning with these access rights, the Model Rules go further by categorically separating digital assets from PDRs, providing a unified sequencing rule for mixed accounts, and explicitly regulating generative AI systems aiming to represent the deceased.
UK/Common Law	Contract/property	No recognised post-mortem privacy. Platform terms generally dictate outcomes. ¹⁰ Digital assets recognised as property under Property (Digital Assets etc) Act 2025	Provides a new framework: Overrides platform terms, establishes statutory succession for digital assets, and guarantees access rights for PDRs.
Model Rules Framework	<i>Sui Generis</i> (Chapters 2 & 3)	Two-regime approach	Assets pass via succession; PDRs are strictly governed by a safeguarded access right, preventing the commodification of digital identity. ¹¹

7. Key Operational Definitions (Article 2(5)–(7))

- **Digital Succession:** Clarifies that the Rules do not rewrite substantive succession law but require digital assets to be administered in

accordance with the applicable law governing movable property.

- **Access Right:** This is defined broadly. It is not a mere right to 'view'. It includes the power to

⁹ LOIn° 2016-1321 du 7 octobre 2016 pour une République numérique; Candice Bordes, Prévoir sa mort numérique. Le devenir des données numériques post-mortem, RDLF 2020 chron. n°09; See Francesco Paolo Patti/Francesca Bartolini, digital inheritance and postmortem data protection: the Italian reform, Number 3397974, June 2019, p. 1; Tribunale di Milano, 10 February 2021, Giurisprudenza italiana, 2022, No. 6, 1363; Tribunale di Bologna, 25 November 2021, De jure, Tribunale di Roma, 10 February 2022. On the last two judgments, see Maniaci, A., d'Arminio Monforte, A., "Eredità digitale" e accesso ai dati personali del defunto, Diritto di Internet, No. 3, 2022, pp. 561-573; Marta Otero Crespo, Post-mortem Data protection and Succession in Digital Assets Under Spanish law, Legal Developments on Cybersecurity and Related Fields, p. 167.

¹⁰ Edina Harbinja, Digital Death, Digital Assets and Post-mortem Privacy: Theory, Technology and the Law (2022).

¹¹ Edina Harbinja, Post-mortem Privacy 2.0: Theory, Law, and Technology, 31 International Review of Law, Computers 26 (2017); Lilian Edwards/Edina Harbinja, Protecting Post-mortem Privacy: Reconsidering The Privacy Interests of The Deceased in a Digital World, 32 Cardozo Arts & Entertainment 83 (2013); Edina Harbinja, Regulating Digital Immortality (Edward Elgar, 2026, forthcoming).

access, rectify, copy, transfer, and delete the content of personal digital remains, bounded by the deceased's directives and third-party protection.

- **Beneficiaries:** Links directly to the exhaustive list in Chapter 3, creating certainty for service providers, executors and administrators regarding exactly who possesses the legal standing to exercise the access right.

export digital assets in an appropriate format before discontinuing a service.

3. Any term in a service provider's terms and conditions that purports to prevent or hinder the transfer of digital assets in accordance with this Article will be invalid unless it was individually negotiated with the deceased. The service provider shall bear the burden of proving that any such clause was individually negotiated with the user.

4. Where no service provider is involved, the person who controls the medium on which the digital asset is recorded must enable the digital asset to be transferred.

Chapter 2

Digital Succession

Article 4 Digital succession

- 1. Digital succession shall be governed by the rules that the law of succession prescribes for succession to movable property, with such modifications as may be necessary to give effect to the nature of the digital assets.**
- 2. Service providers must ensure the orderly transfer of digital assets by:**
 - a. providing mechanisms to enable such transfer in accordance with applicable succession laws;**
 - b. providing clear, accessible, and enforceable tools or platform rules; and**
 - c. issuing adequate prior notice and allowing representatives of the estate to**

1. Core Principle: Succession Neutrality (Article 4(1))

Article 4 affirms a central and broadly accepted inheritance principle: digital assets form part of the deceased's estate and pass under the ordinary rules governing succession to movable property, subject to necessary adaptations to reflect their digital nature.¹² This characterisation of digital assets as movable property applies where the digital asset represents or relates to an underlying immovable asset. In such cases, the rules governing succession to immovable property should prevail. This will necessarily be the case, for example, in situations involving the tokenisation of real estate, where the digital representation ultimately derives its legal significance from the underlying immovable asset.

This rests on a foundational private law doctrine of 'succession neutrality'. Upon death, the inheritable rights and obligations of the deceased transfer to heirs or estate representatives, irrespective of their doctrinal classification (property, contractual claims, intellectual property).¹³ Digital form does not alter this principle. If an interest is capable of control and transfer during life, and is not indissolubly linked to

¹² Julia S. Kharitonova, Digital Assets and Digital Inheritance, Law & Digital Technologies, Vol 1 2022, No 12.

¹³ Michael Birnhack/Tal Morse, Digital remains: property or privacy?, International Journal of Law and Information Technology, 2022, 30, p. 281; Viarengo Ilaria/Re Jacopo, Managing cross-border "digital succession" in the digital era: preliminary remarks on the new challenges for the current legal framework, EU and comparative law issues and challenges series (ECLIC), p. 42; Julia S. Kharitonova, Digital Assets and Digital Inheritance, Law & Digital Technologies, Vol 1 2022, N 12; Edina Harbinja, Digital Death, Digital Assets and Post-mortem Privacy: Theory, Technology and the Law (2022).

the deceased's personality, there is no principled justification for excluding it from succession merely because it is stored electronically.¹⁴

Article 4, therefore, does not create a new category of succession. It confirms inclusion of digital assets within the estate. The 'modifications' referenced in Article 4(1) concern practical administration rather than doctrinal transformation (eg, technical access procedures, export formats, or credential-based recovery).¹⁵ This provides vital legal certainty, especially for European countries that do not currently possess explicit legislation recognising succession to digital assets.¹⁶ Conversely, interests that are inherently personality-bound (Personal Digital Remains) fall strictly outside Article 4 and are governed by Chapter 3, thereby preserving doctrinal coherence.¹⁷

2. Operational Obligations of Service Providers (Article 4(2))

Even where succession law clearly transfers ownership of a digital asset, heirs frequently lack the passwords, authentication tokens, encryption keys, or recovery phrases needed to claim it. Without provider cooperation, the digital asset may be effectively unusable.¹⁸

Article 4(2) recognises that because digital assets are mediated through contractual platforms, effective succession requires structured cooperation. It shifts a

functional obligation onto service providers to ensure transfers are practicably achievable. This obligation is procedural rather than strictly technological. It does not require providers to compromise encryption architectures, but it requires them to design workable, transparent estate-access frameworks.

Furthermore, where services are subject to discontinuation, Article 4(2)(c) requires providers to issue adequate prior notice and allow estate representatives to export digital assets in a commonly used, machine-readable format. This reflects broader European regulatory logic in consumer digital content law, ensuring that succession is not rendered illusory by technical barriers or strategic service termination.¹⁹

3. Contractual Mediation and Invalidation of Non-Transfer Clauses (Article 4(3))

A defining feature of digital assets is their contractual origin. In some jurisdictions, like Germany, heirs 'step into the shoes' of the deceased under national succession law, subject to the terms of the contract. However, many platforms rely on standard Terms of Service that contain boilerplate clauses that automatically terminate accounts upon death or prohibit transfers to heirs.

If such clauses were systematically enforced, succession law could be entirely undermined by unilateral private ordering. In comparative debates, it has been forcefully argued that preventing heirs

¹⁴ Viarengo Ilaria/Re Jacopo, Managing cross-border "digital succession" in the digital era: preliminary remarks on the new challenges for the current legal framework, EU and comparative law issues and challenges series (ECLIC), p. 42; Minnig/Viertler, E-Mail-account-Vertrag und « digitaler Erbgang » – Grundfragen der internationalen Zuständigkeit und des anwendbaren Rechts, in Stephanie Hrubesch-Millauer/Stephan Wolf/Martin Eggel (Hrsg.), Digitales Erbrecht – Perspektiven aus der Schweiz, Bern 2021, p. 222; Edina Harbinja, Digital Death, Digital Assets and Post-mortem Privacy: Theory, Technology and the Law (2022).

¹⁵ Edina Harbinja, Digital Death, Digital Assets and Post-mortem Privacy: Theory, Technology and the Law (2022); Julia S. Kharitonova, Digital Assets and Digital Inheritance, Law & Digital Technologies, Vol 1 2022, No 12; Michael Birnhack/Tal Morse, Digital remains: property or privacy? International Journal of Law and Information Technology, 2022, 30, 281.

¹⁶ Minnig/Viertler, E-Mail-account-Vertrag und « digitaler Erbgang » – Grundfragen der internationalen Zuständigkeit und des anwendbaren Rechts, in Stephanie Hrubesch-Millauer/Stephan Wolf/Martin Eggel (Hrsg.), Digitales Erbrecht – Perspektiven aus der Schweiz, Bern 2021, p. 222 ss.

¹⁷ Viarengo Ilaria/Re Jacopo, Managing cross-border "digital succession" in the digital era: preliminary remarks on the new challenges for the current legal framework, EU and comparative law issues and challenges series (ECLIC), p. 42.

¹⁸ See eg cases summarised in Y. Mandel, 'Facilitating the Intent of Deceased Social Media Users' (2018) 39 Cardozo Law Review 1909, 1910-1912, and results of a survey of 507 estate practitioners, finding that their clients frequently report difficulties accessing digital remains (which they call digital assets): J. D. Michels, S. Hartung, C. Millard, 'Digital Assets: A Call to Action' (London: STEP, 2021) 13, at <<https://www.step.org/research-reports/digital-assets-call-action>>.

¹⁹ Commission Decision (EU) 2025/628 of 31 March 2025 laying down internal rules concerning the provision of information to data subjects and the restrictions of certain data-subjects' rights in relation to the processing of personal data by the Commission for the purpose of the supervision, investigation, enforcement and monitoring under Regulation (EU) 2022/2065.

from accessing inheritable economic assets violates the *ordre public* (public policy) by frustrating estate administration.²⁰

Article 4(3) introduces a calibrated safeguard: non-transfer clauses embedded in standard; non-negotiated terms are legally invalid. The Rules do not call for a blanket invalidation of *all* restrictive clauses; they distinguish between genuine contractual autonomy and provider-imposed limitations. Clauses individually negotiated with the deceased remain valid. Given the severe evidentiary asymmetry between grieving heirs and global tech platforms, the service provider bears the burden of proving that a clause was individually negotiated.

4. Hardware, Third-Party Storage, and the ‘Medium’ (Article 4(4))

The digital nature of assets introduces practical distinctions regarding physical storage. Article 4 must be applied across two distinct hardware scenarios:

- **Scenario A: Medium owned by the deceased.** Where digital assets are stored on a physical device belonging to the deceased (eg, a personal laptop or hardware crypto-wallet), both the medium and the digital asset transfer directly to the heirs.²¹ Access credentials required to use the asset are often already present on the device.
- **Scenario B: Medium controlled by a third party.** A more complex situation arises when the digital asset is stored on infrastructure *not* owned by the deceased (eg, employer-issued devices, institutional servers, or enterprise workspaces) or when the deceased left a laptop to someone but granted access rights to someone else. Here, heirs do not automatically obtain control of the hardware, even though the digital asset itself belongs to the estate.²² Article 4(4) explicitly addresses this gap. The person controlling the medium must enable the transfer of the digital

asset (eg, by exporting the specific files). This does not require surrendering the device itself. It strictly balances estate rights against the owner’s rights in the medium, ensuring that trade secrets, employer confidentiality, and third-party data protection are respected.

5. Intellectual Property and Mixed Cases

Many digital assets embody copyright-protected works. Intellectual property law governs the subsistence, ownership, and duration of their rights. Article 4 does not modify IP doctrine; it simply ensures that platform mediation does not obstruct the lawful transmission of inheritable IP rights to heirs.

However, Article 4 must be read in conjunction with Article 3. A digital asset (such as a copyrighted manuscript) may coexist with personal digital remains (such as sensitive third-party correspondence) within a single record or environment. In such cases, the access-first sequence applies. The exclusion of personal digital remains from the definition of digital assets ensures that identity-bearing material is not automatically absorbed into the property-based succession regime without appropriate privacy filtering.

6. Illustrative Examples

- **Example 1 — Crypto-wallet on a platform:** A deceased holds transferable crypto-assets in an exchange account. The assets pass under the succession law. Under Article 4(2), the provider must facilitate the heirs’ recovery and export of the assets.
- **Example 2 — Monetised platform account:** An online creator account (eg influencer, celebrity) generating income is inheritable. Under Article 4(3), the provider cannot rely on boilerplate Terms of Service to extinguish the asset and deny the heirs the generated revenue.

²⁰ Peyrot Aude/Antreasyan Sevan, Successions 2.0: les biens numériques, Notalex 1/16 p. 20, p. 29.

²¹ Ibid.

²² Marino, M., La successione digitale, Osservatorio del diritto civile e commerciale, No. 1, 2018, pp. 167-204, 182-183.

- **Example 3 — Business data recorded on employer hardware:** A deceased consultant stores proprietary digital assets (to which they own the rights) on a work-issued laptop. Under Article 4(4), the employer (who controls the medium) must enable the extraction of the deceased's transferable digital assets, while maintaining control of the laptop to safeguard confidential employer data.

- **Example 4 — Mixed Records and the 'Ancillary' Test:** A deceased leaves behind two different digital items that qualify as digital assets, but both contain personal data.

(a) *Ancillary Personal Data:* The deceased owned a highly valuable, registered commercial domain name. The registrar's database contains the deceased's personal name, home address, and private phone number. Because this personal data is merely administrative and incidental to the underlying property right, the 'ancillary' exception applies. The domain name passes directly to the heirs under Chapter 2 succession without triggering the Chapter 3 access-first regime.

(b) *Non-Ancillary Personal Data (Mixed Case):* The deceased leaves a monetised, copyrighted blog draft stored on a publishing platform. While the copyright and the revenue stream are transferable digital assets, the draft itself contains highly sensitive, unpublished personal medical data about the deceased and a living relative. Because this personal data is central to the text rather than merely ancillary, it constitutes a true 'mixed case'. The access-first sequence applies: beneficiaries must be allowed to exercise their Chapter 3 rights (eg, redacting or deleting the sensitive medical data to protect privacy) *before* the underlying economic asset (the blog's copyright and publishing rights) transfers to the successors under Chapter 2.

Chapter 3

Deletion of, and Access to, Personal Digital Remains

Article 5 Deletion

The deceased may direct that all or any of their personal digital remains held by a service provider with whom the deceased had an account, or by the person who controls the medium on which the personal digital remains are recorded, shall be deleted.

Article 6 Access right

1. Personal digital remains that have not been deleted in accordance with the directions of the deceased are subject to a right of access by the beneficiaries listed in Article 7.
2. The beneficiaries may exercise the right of access against the service provider with whom the deceased had an account, or where no service provider is involved, against the person who controls the medium on which the personal digital remains are recorded.
3. Any right of access to personal digital remains or right to require their continued preservation shall expire after ten years from the date of the deceased's death.
4. During the period referred to in paragraph 3, service providers and persons who control the medium on which the personal digital remains are recorded shall not charge a fee for the exercise of the access right or the right to require preservation under this Chapter.
5. Any term in a service provider's terms and conditions that purports to prevent or hinder access or compliance with directions

given in accordance with this Chapter will be invalid unless the term was individually negotiated with the deceased. The service provider shall bear the burden of proving that any such term was individually negotiated with the user.

Article 7 *Beneficiaries of the access right*

1. Access to personal digital remains is granted to the following beneficiaries:
 - a. persons explicitly designated by the deceased;
 - b. where the deceased has died intestate, the heirs under the applicable laws of succession (provided that the heir is not the State or an administrative unit);
 - c. where the deceased has left a valid will, the universal heirs or residuary beneficiaries of the estate; and
 - d. executors or administrators of the estate.
2. Where the deceased has designated a person to exercise the access right in respect of all or specified personal digital remains, the beneficiaries listed in paragraph 1(b)–(d) shall not be entitled to exercise the access right in respect of those personal digital remains, except insofar as access is necessary for the settlement of the deceased's estate.
3. The deceased may exclude or limit access to personal digital remains by the beneficiaries listed in paragraph 1.
4. Exclusions or limitations must:
 - a. be specific in scope; and
 - b. clearly identify the personal digital remains affected.
5. Personal digital remains shall not be modified or deleted under this Article, and access to them shall not be excluded or limited under this Article or Article 8, insofar as access to them by the representatives of the deceased's estate is necessary for the settlement of the deceased's estate.
6. Personal digital remains shall not be modified or deleted under this Article, and access to them shall not be excluded or limited under this Article or Article 8, to the extent that such modification or deletion or exclusion or limitation of access would be incompatible with the rights of a third party.
7. Where there are multiple beneficiaries under this Article, and the deceased has not given any other directions, none of the beneficiaries is entitled to delete or modify any personal digital remains unilaterally. If a beneficiary unreasonably refuses to consent to the deletion or modification of personal digital remains, the other beneficiaries may bring the matter before a court to obtain a decision in lieu of unanimous consent.

Article 8 *Directives, methods and priority*

1. The deceased's directives under Articles 5, 6 and 7 (deletion, designation, exclusion or limitation) may be issued through:
 - a. testamentary dispositions;
 - b. an online tool provided by the service provider that also records the date of the directive; and
 - c. a written statement directed to the service provider or the person who controls the medium on which the personal digital remain is recorded.
2. Where the deceased has given more than one designation of a beneficiary and/or more

than one directive, and the designations and/or directives are not consistent with each other, the most recent designation or directive prevails, provided that the date of its making can be reasonably established. Nothing in this paragraph affects the formal validity of a testamentary disposition under the applicable succession law.

3. **Service providers must act in reliance on the latest designation or directive made via the online tool unless they are informed of a later designation or directive within six months after death.**

Article 9 Preservation and exceptions

1. **During the first five years following death, a service provider must preserve personal digital remains to enable access under this Chapter unless:**
 - a. **the deceased gave directions for or explicit prior consent to deletion, either by an individually negotiated term or by means described in Article 8(1); or**
 - b. **the beneficiaries submit a request for modification or deletion of the personal digital remains in accordance with Article 7 paragraph 7.**
2. **After five years, service providers, and other persons who control the medium on which the personal digital remains are recorded, may**

delete personal digital remains unless they have received a request for their continued preservation by a beneficiary under Article 7, or they have been given notice of a legitimate claim to access the content of the remains by a third party in accordance with Article 10.

1. The *Sui Generis* Access Right and the Governance Gap (Articles 5 and 6)

Personal digital remains – encompassing personal communications, images, and identity representations (including AI chatbots) – do not fit neatly into traditional concepts of inheritable property. As outlined in the Introduction and Chapter 1, PDRs are intrinsically tied to the autonomy, intimacy, and identity of the deceased.²³

Applying ordinary succession law to PDRs would risk commodifying deeply personal material and exposing third-party communications inappropriately. Conversely, if heirs and designated beneficiaries are systematically denied all access, legitimate interests – such as estate administration, family memory preservation, and protection against identity misuse – are unprotected.²⁴ Furthermore, while the EU Charter of Fundamental Rights protects privacy and personal data, the GDPR explicitly excludes deceased persons from its scope (Recital 27), leaving a significant regulatory gap across Europe.²⁵

Chapter 3 responds to this gap by establishing a *sui generis* right of access to PDRs. This right is completely distinct from the property-based digital succession governed by Chapter 2. It operates as a regulated gateway, permitting lawful access, preservation, and deletion without conferring ownership or patrimonial rights. This ensures that identity-linked materials are governed by a framework designed to preserve dignity, rather than being treated as inheritable chattels.

²³ Julia S. Kharitonova, Digital Assets and Digital Inheritance, Law & Digital Technologies, Vol 1 2022, N 12; Michael Birnhack/Tal Morse, Digital remains: property or privacy? International Journal of Law and Information Technology, 2022, 30, 281.

²⁴ See Michael Birnhack/Tal Morse, Digital remains: property or privacy? International Journal of Law and Information Technology, 2022, 30, 295; Edina Harbinja, Post-mortem privacy 2.0: theory, law, and technology, 31 International review of law, computers 26 (2017); Lilian Edwards/Edina Harbinja, Protecting post-mortem privacy: reconsidering the privacy interests of the deceased in a digital world., 32 Cardozo arts & entertainment 83 (2013); G. Malgieri, 'R.I.P.: Rest in Privacy or Rest in (Quasi) Property?' in R. Leenes, R. van Brakel, S. Gutwirth, P. de Hert (eds), Data Protection and Privacy: The Internet of Bodies (Oxford: Hart Publishing, 2019) 143.

²⁵ Ondrej Hamulak/Tanel Kerikmäe/Hovsep Kocharyan, The Contemporary Issues of Post-Mortem Personal Data Protection in the EU After GDPR Entering into Force, CYIL 11 (2020), p. 226; CJEU, Case C-101/01 Lindqvist, ECLI:EU:C:2003:596, para 98.

2. Autonomy, Directives, and Priority (Articles 5 & 8)

The deceased's autonomy is paramount. Article 5 affirms that the deceased may direct the absolute deletion of their PDRs. This reflects a core value in European privacy and personality jurisprudence: personal data and digital expressions of identity may continue to "speak" after death in ways that affect dignity and reputation, and individuals must retain control over this.²⁶

Article 8 recognises that modern individuals express their digital wishes through various channels: testamentary dispositions (wills), online tools provided by service platforms (eg, legacy contact features), or written statements.

Where conflicting directives exist, Article 8(2) establishes a strict priority rule: the most recent designation or directive prevails, provided its date can be reasonably established. This date requirement is not a new formal validity condition for wills under national succession law. It operates solely as a priority mechanism to resolve inconsistencies. If the date of the signing of a will cannot be established, it cannot displace a dated online tool directive. This ensures operational certainty for service providers, who must act in reliance on the latest online tool directive unless informed of a later valid instruction within six months of death.

3. Beneficiaries and the Hierarchy of Access (Article 7)

Article 7 provides an exhaustive, hierarchical list of beneficiaries entitled to exercise the access right. Unlike digital assets, which pass automatically to successors, access to PDRs raises serious privacy and third-party concerns and must be strictly limited.

- **The Primacy of Designation (Article 7(1)(a) & 7(2)):** Persons explicitly designated by the deceased occupy the highest position. Crucially, Article 7(2) provides that if the deceased designates a specific person to exercise the

access right, all other heirs and executors are pre-empted and denied access to those specific PDRs, except where strictly necessary to settle the estate. This operationalises informational self-determination, allowing individuals to separate their economic succession from their private digital life.

- **Heirs and Executors (Article 7(1)(b)-(d)):** In the absence of designation, the Rules fall back on universal/residuary heirs and executors. Legatees (beneficiaries of specific assets) are deliberately excluded to prevent disproportionate intrusion into private communications unrelated to their specific bequest.
- **Exclusion of the State:** Where the State or its administrative unit is the ultimate heir on intestacy, it is expressly denied the access right (Article 7(1)(b)). This deliberate policy choice prevents the automatic transfer of intimate digital archives to public authorities, avoiding mass post-mortem surveillance risks.
- **Multi-Beneficiary Governance:** Where multiple beneficiaries exist, Article 7(7) prohibits unilateral deletion or modification, requiring consensus or judicial resolution to prevent the irreversible loss of family memories or reputational damage.

4. Temporal Limits: Preservation vs. Expiration (Articles 6(3), 6(4) & 9)

A critical structural feature of Chapter 3 is the deliberate distinction between the regulatory obligation imposed on service providers (Article 9) and the substantive legal right of access (Article 6).

- **The Five-Year Mandatory Preservation (Article 9(1)):** To prevent 'silent loss', service providers must preserve PDRs for five years following death (unless directed to delete them). This guarantee heirs a reasonable window to locate the will and submit valid access requests.

²⁶ Debie S., Social Mediatisation after Death, in Kerckaert, J., Geiregat, S. (Editors) Social Media Influencers and the Law; KU Leuven 2024; pp. 368 ff.

- **The Ten-Year Absolute Expiration (Article 6(3)):** Compelling platforms to act as indefinite archives imposes disproportionate commercial burdens and severe data security vulnerabilities. Furthermore, in European legal traditions, the protective interest in a deceased person's privacy naturally diminishes over time. Aligning with post-mortem data protection limits in States such as Denmark and Estonia,²⁷ Article 6(3) establishes a strict ten-year expiration of the access right.
- **The Interplay:** From years zero to five, the provider must preserve the data. From years five to ten, the provider may delete the data unless a beneficiary has specifically requested continued preservation. At year ten, the legal right to access permanently expires, ensuring definitive closure. Under Article 6(4), service providers may not charge a fee for facilitating this access or preservation.

5. Third-Party Rights and Contractual Overrides (Articles 6(5), 7(5) & 7(6))

As further detailed in **Chapter 4**, the access right cannot override the fundamental privacy rights of living third parties. Article 7(6) explicitly prohibits modifying, deleting, or accessing PDRs if doing so would be incompatible with third-party rights.

However, service providers cannot use standard Terms of Service to arbitrarily block legitimate access. Mirroring the rule for digital assets in Chapter 2, **Article 6(5)** invalidates any platform terms that purport to prevent or hinder the access right, unless the provider can prove the term was individually negotiated with the deceased.

6. Illustrative Examples

- **Example 1 – Family photographs in a cloud account:** A deceased person's cloud account

contains family photographs featuring living persons. If no deletion directive exists, beneficiaries may access and download them. However, third-party data protection principles (pursuant to the GDPR) apply to any further public disclosure or sharing. The succession regime then applies where there is copyright in photos, and they are treated as digital assets.

- **Example 2 – Email account with legal dispute correspondence:** An email account is a PDR governed by the access regime. However, under Article 7(5), executors are explicitly granted permission to access necessary correspondence to settle the estate, bypassing general exclusions, while GDPR safeguards apply to the third-party data within those emails. Any copyrighted material contained in the account may then pass to successors (eg poems, stories, an unpublished book).
- **Example 3 – A deadbot** trained by the deceased while alive and left 'existing' in the service provider account: see the solution provided in the Introduction.
- **Example 4 – An active dating app account** containing private matches, location data, and highly intimate correspondence: this account is strictly classified as a PDR. It cannot be inherited as a digital asset. If the deceased left a directive to delete the account, the provider must comply immediately. If no directive exists, the beneficiaries may exercise their access right to request the deletion or closure of the account to protect the deceased's post-mortem dignity and privacy. However, under Article 7(6), the beneficiaries would generally be prohibited from reading the actual messages, as doing so would severely infringe upon the fundamental privacy rights of the living third parties (the matches).

²⁷ Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act) (Act No. 502 of 23 May 2018) (Denmark); Hungarian National Data Protection Act XXXVIII (2018) (Hungary); Article 78(7) of Slovak Act No. 18/2018 z. z., On Protection of Personal Data and on Changing and amending of other acts (Slovakia); Portugal, Lei 58/2018 de execução do RGPD, art. 17 (Portugal); Bulgarian Personal Data Protection Act (Bulgaria).

- **Example 5 – Conflict between siblings:** Two heirs disagree about whether to delete a social media profile. Under Article 7(7), neither can act unilaterally. If one unreasonably refuses to consent to deletion, the other may petition the court for a decision in lieu of unanimous consent.

shall, upon request of the third party, exclude or limit access or cease preservation provided that reasons are given in writing and, where contested, the measure is subject to judicial review.

4. **These rules apply without prejudice to any rights the third party may have under data protection law or any other law.**

Chapter 4

Third-party Rights and Interests

Article 10 *Third-party rights and interests*

1. **A third party who demonstrates a legitimate interest (eg because of ongoing legal proceedings or contractual obligations) shall have a right to request access to the content of digital remains from a successor to the digital asset under Chapter 2 or a beneficiary under Chapter 3.**
2. **A third party who demonstrates that continued access to or preservation of digital remains would infringe their rights shall have a right to request deletion, exclusion, or limitation of access to digital remains from a successor to the digital asset under Chapter 2 or a beneficiary under Chapter 3. The measure requested shall be proportionate to the risk that continued access to, or preservation of, the digital remains would pose to third-party rights.**
3. **Where an heir or a beneficiary fails to comply with a request under paragraph 2, and where continued retention of the digital remain would seriously and disproportionately infringe third-party rights, a service provider**

1. The Relational Nature of Digital Remains (Article 10)

As highlighted in the Introduction, digital environments are deeply relational. Digital remains are rarely unilateral records; most digital content is co-produced.²⁸ An email exchange contains at least two data subjects. A shared cloud folder may contain multiple contributors. A joint bank contract may be digitally stored under a single account holder's credentials.

If post-mortem access were limited strictly to successors (under **Chapter 2**) and designated beneficiaries (under **Chapter 3**), significant injustice could result. Third parties might be unable to defend contractual claims, retrieve jointly owned content, or – conversely – protect their own highly sensitive private communications from exposure to the deceased's heirs. Article 10 completes the Model Rules' architecture by introducing a robust, mediated framework to protect these living third parties.

2. The Dual Capabilities: Access vs. Deletion (Articles 10(1) & 10(2))

The Model Rules adopt a balanced model that grants third parties two distinct, judicially reviewable capabilities:

- **The Right to Request Access (The 'Offensive' Right – Article 10(1)):** A third party who demonstrates a legitimate interest under applicable law may request access to the content of digital remains through beneficiaries.

²⁸ Birnhack M., Morse T., Digital remains: property or privacy? in: International Journal of Law and Information Technology, Vol. 30, 2022, p. 288, 290.

The term “legitimate interest” is intentionally broad but requires concrete substantiation before a court: mere curiosity or emotional desire does not suffice.²⁹ Legitimate interests may include defending contractual rights, determining the composition of the estate, accessing hereditary health information, or securing evidence for litigation, depending on the applicable national law. This aligns with, and expands upon, comparative legislative models in Italy and Spain, which recognise access rights for family members or those with legally worthy interests.³⁰

- **The Right to Request Deletion or Limitation (The ‘Defensive’ Right – Article 10(2)):** Conversely, a living third party may demonstrate that continued access to, or preservation of, the remains by the heirs would infringe their rights (eg, an unwarranted invasion of privacy through access to an intimate chat log). The third party may request the deletion, exclusion, or limitation of access to those remains. Because European constitutional frameworks place a strong emphasis on human dignity and privacy,³¹ this defensive measure must be assessed through a strict proportionality test: Is the requested measure necessary? Can redaction suffice? Would deletion disproportionately hinder the administration of the estate?

In legal systems where the protection of third parties in relation to digital assets is structured around a system of publicity rather than one based on control, access to such assets by third parties who demonstrate a legitimate interest or hold rights in respect of them should be facilitated through the institution responsible for ensuring the publicity of those assets in a digital form (eg registry authorities or similar public institutions entrusted with maintaining registries).

3. The Two-Tiered Enforcement Structure (Article 10(3))

Article 10 governs how these third-party rights are enforced, balancing the estate’s autonomy with the privacy of the living, deliberately avoiding turning tech platforms into the primary adjudicators of complex legal disputes.

- **First Tier (Mediation):** Under paragraphs 1 and 2, third parties must initially request access or deletion directly from the successors or beneficiaries. This preserves the two-category architecture established in **Chapter 1** and ensures that the person holding post-mortem authority remains responsible for processing decisions.
- **Second Tier (The Provider Safety Valve):** Recognising that heirs may act maliciously or negligently regarding third-party privacy, Article 10(3) creates a powerful exception. If an heir unjustifiably refuses a request for deletion or limitation, the third party is not left powerless. Where continued retention would ‘seriously and disproportionately infringe’ their rights, the third party may petition the service provider directly to intervene and cut off access. Because this bypasses the heir’s standard rights, it is subject to strict procedural safeguards: it requires a high threshold of harm, written justification by the provider, and is expressly subject to judicial review.

4. Data Protection Continuity and the Household Exemption (Article 10(4))

Article 10(4) explicitly clarifies that death does not extinguish data protection obligations. If heirs or beneficiaries process third-party data found within the digital estate, they must fully comply with

²⁹ P. Meier, *Protection des données: Fondements, principes généraux et droit privé*, Berne, 2011, p. 176, No 343 ff; Rosina Elsa De rosa, *La trasmissibilità mortis causa dei dati digitali*, *Famiglia, Il diritto della famiglia e delle successioni in Europa*, p. 3.

³⁰ Garante per la protezione dei dati personali, *Accesso ai dati di persona deceduta*, in *Bollettino* no. 27, p. 20; Spanish Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights; Marta Otero Crespo, *Post-mortem Data protection and Succession in Digital Assets Under Spanish law*, *Legal Developments on Cybersecurity and Related Fields*, p. 177.

³¹ O. Hamulak, H. Kocharyan, T. Kerimäe, *The Contemporary Issues of Post-Mortem Personal Data Protection in the EU After GDPR Entering into Force*, in: *Czech Yearbook of Public and Private International law*, Vol. 11, 2020, p. 235.

applicable data protection laws (eg, the GDPR). Third parties retain remedies equivalent to those they possessed while the deceased was alive.

In some cases, heirs may process third-party data for purely personal or household purposes (which falls outside the scope of the GDPR under Article 2(2)(c)). However, once the heirs' processing exceeds private use – for example, publication, disclosure in litigation, or commercial exploitation – data protection obligations under GDPR fully arise.

5. Illustrative Examples

- **Example 1 – Joint bank account dispute (Requesting Access):** A surviving joint account holder requires access to correspondence between the deceased and the bank to resolve contractual liabilities. The interest is legal and financial. Access may be granted proportionately under Article 10(1).
- **Example 2 – Genetic medical information (Requesting Access):** A child seeks access to medical correspondence stored in the deceased's cloud account to determine a serious hereditary disease risk. The interest is compelling and health related. Limited, proportionate access may be justified under Article 10(1).
- **Example 3 – Protecting Private Correspondence (Requesting Deletion/Limitation):** The deceased's heirs gain access to a messaging or dating app containing highly intimate communications from a living third party. Fearing the heirs will read or publish the messages, the third party requests that the heirs delete or restrict access to that specific chat log under Article 10(2) to protect their privacy.
- **Example 4 – Service Provider Intervention:** Following Example 3, the heirs refuse to delete the intimate messages. The third party proves that the heirs intend to publish them, which would seriously and disproportionately infringe their right to privacy. Under Article 10(3), the third party requests the service provider to lock the specific chat log. The provider complies, documenting the reasons in writing and bypassing the heirs' access.

Chapter 5

Applicable Law and Jurisdiction

| Article 11

1. **These Model Rules apply without prejudice to applicable EU or national private international law rules, in particular those concerning applicable law and jurisdiction in matters of digital succession or access rights to personal digital remains.**
2. **For non-EU countries: These Model Rules apply without prejudice to applicable national private international law rules, in particular those concerning applicable law and jurisdiction in matters of digital succession or access rights to personal digital remains.**

1. Preliminary: A System-Integrated Approach to Private International Law

As outlined in the Introduction, this option adopts a structurally conservative and system-integrated approach. Rather than creating an autonomous private international law regime or introducing overriding mandatory provisions (*lois de police*) for digital remains, Chapter 5 explicitly embeds the Model Rules within the existing, sophisticated framework of European private international law (Article 11(1)). For non-EU countries, the same principle applies with respect to national private international law (Article 11(2)).

This approach reflects the premise that digital assets and personal digital remains do not constitute a completely new juridical category requiring separate conflict rules.

Consequently, Chapter 5 clarifies, in a declaratory manner, that the Model Rules do not prejudice the application of EU and/or national private international law rules. Those rules therefore apply to digital succession and to related contractual relationships between the service provider and the heirs, in particular as regards the applicable law and jurisdiction, and even enforcement of decisions on those matters.

As regards EU countries (Article 11(1)), the Model Rules also rely on the existing EU framework and mainly, but not exclusively, on three instruments:

- **Regulation (EU) No 650/2012 (Succession Regulation):** Governs applicable law and jurisdiction for the succession of the estate as a whole (digital or physical);³²
- **Regulation (EC) No 593/2008 (Rome I Regulation):** Governs the law applicable to contractual obligations;³³ and
- **Regulation (EU) No 1215/2012 (Brussels Ibis Regulation):** Governs jurisdiction in civil and commercial matters.³⁴

Other regulatory instruments – such as the GDPR, the Data Governance Act (DGA)³⁵, and the Digital Services Act (DSA)³⁶ – are relevant but do not provide autonomous conflict-of-laws rules suitable to govern digital succession or post-mortem access. Specifically, Recital 27 of the GDPR excludes the data of deceased persons, meaning no private international law principles for post-mortem access can be derived from it.

For non-EU countries, national private international law rules, on the other hand, determine the applicable law, jurisdiction, and other relevant issues in matters of digital succession or access rights to PDRs (Article 11(2)).

The following section presents the general principles for illustrative purposes.

2. Digital Succession for EU Countries: The Dual Framework (Article 11(1))

As regards digital succession, the Succession Regulation applies, as it governs both physical and digital succession³⁷. Consequently, digital assets (governed by Chapter 2) are subject to the same private international law principles as tangible movable property. However, because digital assets arise through contracts, a dual legal framework applies:

- **The *Lex successionis*:** The Succession Regulation determines the applicable law governing *who* inherits the digital asset. The law of the Member State where the deceased had their habitual residence at death generally governs the entire succession, preserving unity of the estate. If the deceased made a valid choice of law (*professio juris*), that choice extends to the digital assets.³⁸
- **The *Lex contractus* and Jurisdiction:** While succession law determines who steps into the deceased's shoes, the inherited digital asset itself often consists of a contractual relationship (eg, an online bank account or crypto exchange). The applicable law and the jurisdiction of this contractual relationship are governed by other instruments, such as the Rome I and Brussels Ibis. Under Rome I, the law

³² R. E. De Rosa, What Happens to my “digital Heritage” if I Die? Part I, Law and Digital Economy No 1 (15) 2022, p. 37; Daniel Leu/Valérie Humm, Digitaler Nachlass und Willensvollstreckung, in Hans-Daniel Künzle (Hrsg.), 4. Schweizerisch-deutscher Testamentsvollstreckertag, 2021, p. 163; Ilaria Viarengo/Jacopo Re, Managing cross-border “Digital succession” in the digital era: preliminary remarks on the new challenges for the current legal framework, EU and comparative Law Issues and challenges series, p. 41; Francesca Zagaria, Patrimonio digitale e successione mortis causa, De iustitia 2020, p. 10.

³³ Susanne Lilian Gössel, Italienische Netzverträge (contratti di rete), Niederlassungsfreiheit und anwendbares, Rubels Zeitschrift für ausländisches und internationales Privatrecht, Bd. 80, H. 3 (Juli 2016), p. 601; Ilaria Viarengo/Jacopo Re, Managing cross-border „Digital succession” in the digital era, p. 44; Francesca Zagaria, Patrimonio digitale e successione mortis causa, De iustitia 2020, p. 8.

³⁴ BGH, 12.07.2018 – III ZR 183/17; Ilaria Viarengo/Jacopo Re, Managing cross-border “Digital succession” in the digital era, p. 44; Michel Birnhack/Tal Morse, Digital remains: property or privacy? International Journal of Law and Information Technology, 2022, p. 289; Francesca Zagaria, Patrimonio digitale e successione mortis causa, De iustitia 2020, p. 6; Ana Mercedes López Rodríguez, Jurisdiction, Recognition and enforcement of judgments in claims arising out of smart contracts under the Brussels I Regulation (recast) and on the blockchain, Freedom, Security, justice, p. 154; G. Van Calster, European Private International Law, 2nd edn., Oxford, 2016, p. 71.

³⁵ Andrei Mikes/Rita Flakoll, An overview of the EU data governance Act, Clifford Chance, p. 3.

³⁶ Art. 2(1) of the DSA; Dominika Moravcová, Impact of the DSA Regulation on Very Large Online Platforms, Central European Journal of Comparative Law, Volume IV, 2023 (2), p. 166.

³⁷ See note 32.

³⁸ As regards the rules governing the applicable law and jurisdiction in international successions under Regulation (EU) No 650/2012, see Angelika Fuchs, The new EU Succession Regulation in a nutshell, ERA Forum 2015, p. 120-121; Alfonso-Luis Calvo Caravaca/Angelo Davi/Heinz-Peter Mansel (Hrsg.), The EU Succession Regulation, Cambridge 2016, p. 125, 289. For current framework in terms of applicable law in international digital successions matters, see R. E. De Rosa, What Happens to my “digital Heritage” if I Die? Part I, Law and Digital Economy No 1 (15) 2022, p. 37.

chosen in the service provider's Terms of Service generally applies. Under Brussels Ibis, the contract's jurisdiction clause generally applies. The practical consequence is that heirs inherit both the asset *and* the contractual framework within which the asset exists. The Model Rules preserve this distinction rather than merging contractual and succession issues into a single forum. Crucially, however, heirs benefit from existing consumer protection. If the deceased qualified as a consumer, Article 6 of Rome I ensures they cannot be deprived of mandatory local protection, and Article 17 of Brussels Ibis allows heirs to bring proceedings in the courts of the deceased's domicile, bypassing foreign jurisdiction clauses.³⁹

3. Access to Personal Digital Remains for EU Countries: Article 11(1)

Access to PDRs (governed by Chapter 3) is a *sui generis* right. Because PDRs do not generally transfer as property, in particular for legal systems that exclude PDRs as part of the estate, the Succession Regulation cannot apply to them⁴⁰. Instead, access rights are always exercised within a contractual digital environment (eg, a social media platform or cloud service).

Therefore, PDRs access disputes are mainly aligned with the Rome I and Brussels Ibis framework. Beneficiaries exercising access rights step into the deceased's contractual position solely for the purpose of executing the access right. The governing law and jurisdiction clauses in the service provider's contract apply, subject to the consumer protection safeguards mentioned above (Articles 6 of Rome I and 17 of Brussels Ibis).

This ensures that beneficiaries are not systematically forced to litigate abroad in consumer contexts, while maintaining absolute coherence with existing EU private international law.

4. Jurisdictions and applicable law not subject to the relevant EU Regulations (Article 11(2))

For cases outside the geographic scope of the relevant EU regulations, or for Member States that have not adopted the full EU framework (for example, Denmark or Ireland in relation to the Succession Regulation), Article 11(2) clarifies that the national rules of private international law apply. This ensures coherence and predictability in cross-border contexts beyond the geographical scope of the relevant EU legislation.

5. Illustrative Examples

- **Example 1 – Digital Bank Account (Digital Asset):** D dies in Spain where they were habitually resident, leaving a digital bank account used for business. The bank is in Lithuania; the contract mandates Lithuanian law and jurisdiction.
 - *Application:* Spanish law (under the Succession Regulation) determines *who* inherits the account. However, because D was using it for business purposes (not as a consumer), Lithuanian law governs the contract (Rome I), and Lithuanian courts hold jurisdiction over contractual disputes (Brussels Ibis). The heirs inherit the asset under Spanish law but must assert their contractual rights in Lithuania.
- **Example 2 – Personal Email Account (Personal Digital Remain):** K dies in France where they were habitually resident, leaving a personal Gmail account stored on a server in Germany. The Terms of Service mandate German law and jurisdiction.
 - *Application:* As a PDR, the Succession Regulation does not apply. The contract is governed by German law (Rome I),

³⁹ Zhen Chen, Jurisdiction and choice of law rules over electronic consumer contracts: The nexus between the concluded contract and the targeting activity, *Maastricht Journal of European and Comparative Law*, 2022, Vol. 29(3), p. 329; Ana Mercedes López Rodríguez, Jurisdiction, Recognition and enforcement of judgments in claims arising out of smart contracts under the Brussels I Regulation (recast) and on the blockchain, *Freedom, Security, justice*, p. 154 s.

⁴⁰ It is specified that, where PDRs are considered part of the estate, they shall be subject to the Succession Regulation in accordance with the principles set out above.

but because K was a consumer, French mandatory protective provisions still apply (Article 6 paragraph 2 Rome I). For jurisdiction, the beneficiaries may invoke Article 17 of Brussels Ibis to bring proceedings regarding their access rights in the French courts, despite the contract's German jurisdiction clause.

6. Summary

This approach does not expand heirs' or beneficiaries' protection beyond the current European private international law framework. Where the deceased validly agreed to foreign governing law or jurisdiction clauses, heirs may be bound by them. Nevertheless, this approach ensures systemic coherence, preserves the unity of succession, respects party autonomy, and leverages existing consumer safeguards without requiring legislative innovation. That said, future legislative developments aimed at strengthening the protection of heirs and beneficiaries may be both feasible and desirable, for example, by introducing mandatory rules on applicable law or jurisdiction in matters of digital succession or access to personal digital remains.

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