European Journal of Risk Regulation (2026), 1–15
doi:10.1017/err.2026.10178

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Exit without Migration: Cloud Switching and Operational Continuity in EU Law

Mahmoud Javadi

Vrije Universiteit Brussel, Belgium
Email: mahmoud.javadi@vub.be

Abstract

EU law can make cloud exit legally enforceable while leaving migration operationally uncertain. This article asks why a customer with a binding right to leave a cloud provider may still lack a workable way to continue the service elsewhere. Reading the EU Data Act alongside the Digital Operational Resilience Act (DORA), it shows how switching and operational continuity depend on conditions governed by different obligations and actors. The Data Act addresses provider-side switching obstacles but bounds the departing provider's responsibility where reconstruction also depends on the customer, the destination environment and differentiated service functionality. In finance, DORA requires financial entities to prepare for continuity of critical or important functions. These limits on provider responsibility can be proportionate, even as migration remains operationally uncertain. The article argues that DORA's existing requirements for feasible, tested and continuity-preserving exit plans should substantiate a credible path for reconstituting and continuing the regulated function after exit. More broadly, it shows how individually defensible regulatory duties can leave a shared operational outcome insufficiently substantiated when responsibility is distributed across instruments.

Keywords: cloud exit; cloud migration; Data Act; DORA; EU risk regulation

I. Introduction

Cloud services have become part of the ordinary infrastructure of European economic and administrative life. European Union (EU) enterprise cloud uptake rose from 34% in 2021 to 46.7% in 2025, against the EU's Digital Decade target of 75% by 2030.[1] This expansion takes place in a market marked by cloud provider concentration and structural dependence. The European Commission has identified cloud as part of Europe's technological dependence problem, noting that three large United States-based cloud service providers hold more than 70% of the EU cloud market and that the share of EU providers fell from 29% in 2017 to 15% in 2022.[2] As cloud use expands under these conditions, EU law increasingly treats switching, portability and exit rights as instruments for reducing dependence.[3]

[1] Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: State of the Digital Decade 2026: Closing Structural Gaps and Mobilising Investments for 2030 and Beyond" COM (2026) 288 final.

[2] Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Tech Sovereignty, Accompanied by an EU Open Source Strategy" COM (2026) 503 final.

[3] Commission, "Cloud Computing" (Shaping Europe's Digital Future, 24 March 2026) <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing>(last accessed 14 October 2026).

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2026.10178

These instruments make departure legally credible while leaving open what happens afterwards. A cloud customer may hold a binding right to leave a cloud provider and still lack an executable basis for continuing the service elsewhere. Ending the relationship and transferring data or digital assets differ from making applications, configurations, security arrangements and service functionality work in another environment. This second task is the *migration* problem, understood here as the reconstitution of a working cloud service after exit. The legal puzzle concerns how law allocates responsibility for the conditions on which migration depends. This gives rise to the article's inquiry: *why, under EU law, can a binding right to exit a cloud service provider leave the customer unable to migrate?*

Existing scholarship has made Europe's cloud dependence visible from several directions. Cloud sovereignty and digital political economy scholarship explains dependence through strategic autonomy, infrastructural power and provider concentration.[4] Financial regulation studies examine cloud concentration as a source of operational and potentially systemic risk.[5] Private law research on cloud contracts addresses technical lock-in alongside contractual allocation, control, security and risk.[6] Data Act scholarship comes closest to the legal problem examined here, analysing cloud switching and interoperability, service-type classification, standardisation, and the difficulty of applying equivalence duties to dynamic and differentiated cloud services.[7] These literatures identify the principal sources of cloud dependence and the difficulties of governing them. They have paid less attention to how different legal regimes allocate responsibility across departure, switching and operational continuity when provider-side portability duties may themselves have defensible limits.

This article examines the allocation directly. It contends that a binding right to exit can leave the customer unable to migrate because departure and service reconstruction depend on different conditions and are allocated across different actors and regulatory techniques. The explanation therefore lies in this allocation of responsibility rather than simply in the absence of stronger portability duties. Provider-side switching rules can make departure legally robust while bounding the departing provider's responsibility where reconstruction also depends on the customer, the destination environment,

[4] See F. G. Blancato, "The Cloud Sovereignty Nexus: How the European Union Seeks to Reverse Strategic Dependencies in Its Digital Ecosystem" (2024) 16 Policy & Internet 12; R. Adler-Nissen and K A Eggeling, "The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X" (2024) 62 Journal of Common Market Studies 993; A. Baur, "European Ambitions Captured by American Clouds: Digital Sovereignty through Gaia-X?" (2026) 29 Information, Communication & Society 417.

[5] See E. Kun, "Challenges in Regulating Cloud Service Providers in EU Financial Regulation: From Operational to Systemic Risks, and Examining Challenges of the New Oversight Regime for Critical Cloud Service Providers under the Digital Operational Resilience Act" (2024) 52 Computer Law & Security Review 105931; N. Remolina, "Addressing Financial Stability in the Era of Cloud Computing" (2026) SSRN Working Paper <https://ssrn.com/abstract=6033774>(last accessed 14 October 2026).

[6] See C. Millard (ed), *Cloud Computing Law* (2nd edn, Oxford University Press 2021).

[7] See S. Geiregat, "The Data Act: Start of a New Era for Data Ownership?" (2022) SSRN Working Paper <https://ssrn.com/abstract=4214704>(last accessed 14 October 2026); D. Schnurr, "Switching and Interoperability Between Data Processing Services in the Proposed Data Act" in J. Krämer (coord), *Data Act: Towards a Balanced EU Data Regulation* (CERRE 2023) <https://cerre.eu/wp-content/uploads/2023/03/230327_Data-Act-Book.pdf>(last accessed 14 October 2026); S. F. Ennis and B. Evans, "Cloud Portability and Interoperability under the EU Data Act: Dynamism versus Equivalence" (2024) SSRN Working Paper <https://ssrn.com/abstract=4395183>(last accessed 14 October 2026); J.-P. Schneider, J. Erny and F. Enderlein, "Collaborative Governance Structures for Interoperability in the EU's New Data Acts" (2025) 16 European Journal of Risk Regulation 24; L. Ott and Y. Dong, "Clouds Connecting Europe: Interoperability in the EU Data Act" (2025) 16 Journal of Intellectual Property, Information Technology and E-Commerce Law 154 <https://www.jipitec.eu/jipitec/article/view/435>(last accessed 14 October 2026); P. Terzis, A. Mittal and J. van Hoboken, "The Many Shades of Clouds: How Law Fails (Us) in Seeing Power in the Digital Economy" (2026) Regulation & Governance <https://doi.org/10.1111/rego.70149>(last accessed 14 October 2026).

https://doi.org/10.1017/err.2026.10178

differentiated functionality or technical conditions beyond its control.[8] Migration difficulty alone provides an insufficient basis for extending the departing provider's responsibility to the reconstruction outcome.

The analysis focuses on EU financial law, where this allocation is structured through two intersecting regimes. The Data Act supplies the horizontal switching regime for customers of data processing services,[9] while the Digital Operational Resilience Act (DORA) governs financial entities' management of information and communication technology (ICT) third-party dependence, including preparation for exit from arrangements supporting critical or important functions.[10] Within finance, DORA places cloud reliance within digital operational resilience, with continuity of critical or important functions itself a legal and supervisory concern. The two regimes also rest on distinct regulatory rationales. Data Act switching rules respond partly to limits of private ordering: integration can raise switching costs, future migratability can be costly to verify, and voluntary arrangements had proved insufficient to remove baseline switching obstacles reliably.[11] DORA adds a prudential rationale because privately chosen exit optionality may fall short of the continuity preparedness required for critical or important functions, particularly where common ICT dependencies create correlated exposure.[12] The article uses doctrinal legal analysis of these regulations, their implementing measures and supervisory evidence. Adjacent regimes addressing other dimensions of cloud dependence remain outside the article's core inquiry.[13]

The article contributes a legal design account of how responsibility is distributed across cloud exit. It shifts the unit of analysis from portability duties in isolation to the allocation of responsibility across instruments for the conditions of migration and continuity. The analysis incorporates proportionality concerns about the burdens expansive equivalence

[8] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L 2023/2854 (Data Act), Arts. 30(1) and (6) and recitals 85, 86 and 92. Recital 85 distributes responsibilities across the switching process, while recital 92 explains that functional equivalence does not require the source provider to rebuild the service in the destination provider's infrastructure.

[9] Data Act, Arts. 23–31.

[10] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1 (DORA), especially Arts. 28–31.

[11] Commission, "Impact Assessment Report Accompanying the Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)" (Commission Staff Working Document) SWD (2022) 34 final, section 2.2, Driver 4.1, section 5.2.4 and Annex 9; Competition and Markets Authority, "Cloud Infrastructure Services: Final Decision Report" (31 July 2025) paras. 6.19–6.24, 6.37–6.38 and 6.53–6.55 <https://assets.publishing.service.gov.uk/media/688b8891fdde2b8f73469544/final_decision_report.pdf>(last accessed 14 October 2026). The European Commission identified contractual, economic and technical switching obstacles and limited uptake of voluntary cloud switching arrangements, while choosing minimum framework conditions rather than the more prescriptive technical option considered in the impact assessment.

[12] Financial Stability Board, "Third-Party Dependencies in Cloud Services: Considerations on Financial Stability Implications" (9 December 2019) 3–4 <https://www.fsb.org/uploads/P091219-2.pdf>(last accessed 14 October 2026); Commission, "Impact Assessment Report Accompanying the Proposal for a Regulation on Digital Operational Resilience for the Financial Sector" (Commission Staff Working Document) SWD (2020) 198 final, 18–19. The Financial Stability Board (FSB) identifies possible negative externalities and collective underinvestment in continuity, contingency, exit preparedness and relevant expertise while also recognising that cloud services can improve institution-level resilience.

[13] Adjacent regimes address different dimensions of cloud dependence and fall outside the direct inquiry. Competition law and the Digital Markets Act address market power and contestability; procurement law structures public sector purchasing; and cloud certification concerns assurance, security and trust. These regimes remain relevant to the wider governance of cloud dependence but do not directly structure the relationship between cloud switching and operational resilience obligations examined here.

https://doi.org/10.1017/err.2026.10178

obligations may impose on dynamic and differentiated cloud services.[14] It applies *instrument reach* as an analytical lens for distinguishing the actor, dependency and outcome governed by different legal duties, and for identifying where responsibility for residual dependence lies when an obligation reaches only part of the operational problem.

The broader implication concerns regulatory architectures in which responsibility for a single operational outcome is distributed across duties with different objects and addressees. Proportionality may justify limits on obligations imposed on one actor while residual risk is governed elsewhere. The legal significance of compliance depends on what each duty is capable of evidencing. Compliance with switching duties can establish that the provider-side conditions governing departure have been satisfied. DORA's exit-planning requirements raise a different evidentiary question: whether the financial entity's preparations substantiate a credible, feasible and sufficiently tested path for reconstituting and continuing the regulated function after exit. In EU financial law, this evidentiary relationship connects the Data Act's bounded switching regime with DORA's continuity objective. The regulatory challenge is to assess each form of compliance according to the operational outcome it can substantiate, without treating completion of one regulatory task as proof of another.

The article proceeds as follows. Section II develops instrument reach and explains why proportionate *ex ante* intervention can be justified while provider-side portability remains bounded, distinguishing the switching rationale from the additional prudential rationale for financial sector resilience. Section III applies this framework to EU financial law, examining DORA's entity-side resilience obligations, the Data Act's provider-side switching regime and Article 30's differentiated treatment of migration conditions. Section IV draws the regulatory consequence by arguing that DORA's existing exit-planning requirements should substantiate a credible, workable and sufficiently tested path for reconstituting and continuing the regulated function after exit.

II. Cloud exit and instrument reach

Exit rights discipline dependence by making departure from a relationship legally credible.[15] In cloud services, however, the legal capacity to leave and the operational capacity to continue elsewhere are distinct. A customer able to terminate a provider relationship gains a protected outside option, but its practical value depends on what must be transferred, replaced or reconstructed before the service can operate elsewhere. The question concerns both the legal strength of an exit duty and the part of the underlying dependence it governs.

Instrument reach describes the part of an underlying dependence governed through a legal mechanism, with attention to its addressee, object and required outcome. Legal instruments differ in what they require, from whom and through which institutional setting; their effectiveness depends partly on the fit between regulatory technique and the problem being governed.[16] An instrument may govern termination, switching charges, provider cooperation, technical transfer or the service outcome after switching, and may operate through a customer-held entitlement, a provider obligation or supervisory

[14] See Ennis and Evans, *supra,* note 7, who argue that expansive cloud portability and equivalence requirements can sit uneasily with dynamic competition, differentiated services and innovation. Their analysis supports treating migration difficulty as insufficient, by itself, to justify universal functional equivalence. The question pursued here is what becomes of continuity risk once provider-side duties are bounded for those reasons.

[15] A. O. Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (Harvard University Press 1970).

[16] R. Baldwin and J. Black, "Really Responsive Regulation" (2008) 71 Modern Law Review 59; R. Baldwin, M. Cave and M. Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, Oxford University Press 2012).

https://doi.org/10.1017/err.2026.10178

oversight. These mechanisms can shape the practical value of exit across different parts of dependence. Assessing an instrument's reach requires attention to regulatory fit, with broader intervention carrying no presumption of superiority. Extending an obligation to conditions outside the regulated actor's control can be difficult to specify and justify. The relevant question is which part of dependence an instrument can appropriately govern and how responsibility for what remains is allocated.

Cloud architecture makes this distinction consequential. Standards, interfaces, system configuration and technical design can structure the practical possibilities of switching alongside the legal terms governing exit.[17] Portability scholarship similarly establishes that a legally protected transfer has limited practical value if what is transferred cannot be effectively used in the receiving environment.[18] Cloud migration extends the problem beyond transfer. Dependence may arise not only from contractual terms, charges and accumulated investment, but also from provider-specific interfaces, managed services, customised applications, configuration and the skills needed to operate them. Migration can consequently involve adaptation, re-engineering and architectural change, including modification or reconstruction of applications for the destination environment.[19] The relevant distinction cuts across cloud service layers, since infrastructure services can also generate lock-in. It separates dependencies addressed through departure and transfer duties from those embedded in the conditions required for the service to operate elsewhere.

Technical integration can change the economic value of the exit option over time. The effective outside option available at initial contracting can deteriorate over the course of a cloud relationship. The UK Competition and Markets Authority (CMA) found that longer use can deepen integration into the hosting cloud and that switching costs vary with source-destination compatibility, workload architecture, data, continuity requirements and available skills. Cloud adoption can require investment in organisational change, complementary services, business-process adaptation, skills, monitoring and contract management.[20] Provider specificity may nevertheless reflect a rational trade-off, with customers accepting weaker future portability in return for differentiated or customised functionality.[21] An initially competitive procurement can be followed by a more costly exit once workloads and operations have adapted to the chosen environment.[22]

[17] J. R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1998) 76 Texas Law Review 553; Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006).

[18] P. de Hert and others, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services" (2018) 34 Computer Law & Security Review 193; I. Graef, M. Husovec and N. Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" (2018) 19 German Law Journal 1359 <https://doi.org/10.1017/S2071832200023075>(last accessed 14 October 2026).

[19] P. Jamshidi, A. Ahmad and C. Pahl, "Cloud Migration Research: A Systematic Review" (2013) 1 IEEE Transactions on Cloud Computing 142; V. Andrikopoulos and others, "How to Adapt Applications for the Cloud Environment: Challenges and Solutions in Migrating Applications to the Cloud" (2013) 95 Computing 493; J. Opara-Martins, R. Sahandi and F. Tian, "Critical Analysis of Vendor Lock-In and Its Impact on Cloud Computing Migration: A Business Perspective" (2016) 5 Journal of Cloud Computing 4 <https://doi.org/10.1186/s13677-016-0054-z>(last accessed 14 October 2026); M. F. Gholami and others, "Challenges in Migrating Legacy Software Systems to the Cloud: An Empirical Study" (2017) 67 Information Systems 100.

[20] R. Makhlouf, "Cloudy Transaction Costs: A Dive into Cloud Computing Economics" (2020) 9 Journal of Cloud Computing 1 <https://doi.org/10.1186/s13677-019-0149-4>(last accessed 14 October 2026); Competition and Markets Authority, *supra,* note 11, paras. 6.37–6.38. Makhlouf identifies transaction costs associated with cloud adoption, including organisational change, complementary services, business-process re-engineering, skills, contract management and monitoring.

[21] See Ennis and Evans, *supra,* note 7.

[22] The switching cost literature explains why competitive conditions at initial contracting do not necessarily determine competitive conditions later in the relationship. Switching costs can make initially substitutable suppliers effectively differentiated after adoption and can give an incumbent greater leverage over an installed customer base. *Ex ante* competition for customers may offset some or all of these effects, however, so the existence

https://doi.org/10.1017/err.2026.10178

Future migratability is only partly foreseeable and can be costly to verify when the relationship begins. Contract terms can specify notice, data-return formats, assistance, charges and other exit conditions. Future workload architecture, destination compatibility, accumulated integrations and reconstruction effort remain partly unsettled at contracting. The CMA found that newer cloud customers may struggle to understand the technical requirements of switching. Concrete obstacles can remain difficult to identify until migration becomes an active exercise; extensive recoding was among the concerns identified once those obstacles were examined more closely.[23] Earlier European Commission-commissioned research likewise found migration difficulty to depend on service type, application and data architecture, interfaces, service requirements and customer capability. The study concluded that large organisations could generally overcome such difficulties, although at a cost.[24] The evidence supports a narrower diagnosis of incomplete foresight and costly verification rather than a general provider-customer information asymmetry.

In market-failure terms, the intervention case rests on more specific frictions than technical dependence or vendor lock-in alone. Integration can weaken competitive discipline after contracting by raising the cost of the customer's outside option;[25] important aspects of future migratability can be costly to verify; and provider incentives to remove switching frictions may be insufficient or mixed. The CMA found providers' incentives to facilitate switching and the use of multiple cloud providers to be mixed, since portability may attract new customers while also strengthening the bargaining position of existing ones.[26] Concentration can amplify these conditions where credible substitutes are limited, but concentration alone does not establish a switching failure. A customer's choice of a less portable architecture likewise provides no basis, by itself, for inferring inefficient underinvestment. The case for provider-side intervention is strongest where private ordering leaves unresolved contractual, economic, procedural or avoidable technical barriers substantially within the source provider's control.

The Data Act's preparatory record reflects this limited rationale. Its impact assessment identified contractual, economic and technical obstacles to switching and recorded very limited uptake of the voluntary cloud switching codes, which were largely confined to pre-contractual transparency and did little to address technical and economic hurdles. The European Commission considered those problems likely to persist absent intervention but selected binding minimum framework conditions rather than the more prescriptive option of generally applicable technical interoperability requirements.[27] The European Commission study had likewise identified weaknesses in voluntary approaches. It found that sophisticated organisations could usually overcome portability problems at a cost and

of switching costs or lock-in does not itself establish inefficiency or justify regulatory intervention. Where such competition does not fully discipline the later relationship, switching costs can impede efficient switching, soften competition and leave *ex post* rents incompletely competed away. See P. Klemperer, "Markets with Consumer Switching Costs" (1987) 102 Quarterly Journal of Economics 375; J. Farrell and P. Klemperer, "Coordination and Lock-In: Competition with Switching Costs and Network Effects" in M. Armstrong and R. Porter (eds), *Handbook of Industrial Organization*, vol 3 (Elsevier 2007) 1967. The narrower point here is that an initially competitive procurement is compatible with a deterioration in the customer's effective outside option over time; it does not follow that every switching cost is inefficient or that regulation should guarantee substitutability.

[23] Competition and Markets Authority, *supra,* note 11, paras 6.37(b), 6.53–6.55.

[24] D. Hayward and others, Switching of Cloud Services Providers: Final Report, SMART 2016/0032 (European Commission 2018) 4–5 <https://doi.org/10.2759/457551>(last accessed 14 October 2026).

[25] See Klemperer, *supra,* note 22.

[26] Competition and Markets Authority, *supra,* note 11, paras 6.23–6.24.

[27] SWD (2022) 34 final, section 2.2, Driver 4.1, section 5.2.4 and Annex 9. The voluntary codes were developed by the European Commission-facilitated Switching Cloud Providers and Porting Data (SWIPO) group. The impact assessment recorded very limited uptake and concluded that the codes remained largely confined to pre-contractual transparency rather than addressing the relevant technical and economic hurdles.

https://doi.org/10.1017/err.2026.10178

recorded concerns that poorly bounded portability duties could impose substantial compliance burdens and impede innovation.[28] The rationale for *ex ante* switching rules is therefore not that law should eliminate provider specificity or guarantee reconstruction. Baseline obligations can instead preserve a more credible exit option by addressing barriers left unresolved by voluntary arrangements.

Financial regulation adds a distinct prudential rationale. DORA places ICT third-party dependence within a broader digital operational resilience framework, where continuity of critical or important functions is itself a regulatory concern. Its impact assessment distinguished ICT third-party risks affecting individual institutions from concentration and potentially systemic risks created by common dependence on a limited number of providers, and identified limits in a supervisory model centred on each institution's contractual arrangements with its suppliers.[29] The Financial Stability Board (FSB) supplies the corresponding incentive logic: cloud services can improve resilience for an individual institution while common third-party dependencies can create additional system-level exposure, including possible negative externalities and collective underinvestment in continuity, contingency, exit preparedness and relevant expertise.[30] This does not establish that sophisticated cloud customers generally underinvest in switching. The evidence supports the narrower conclusion that the privately rational level of exit optionality may fall short of the continuity preparedness required for critical or important functions. This prudential rationale supports DORA's requirement of tested exit preparedness beyond what bilateral contracting alone can be relied upon to secure, without treating every concentrated dependency as systemic or every service as interchangeable.[31]

Instrument reach places these rationales within a common legal design frame that preserves their distinct objects. Provider-side rules can address obstacles substantially controlled by the source provider; entity-side resilience duties can require preparation for dependencies that remain; and interoperability requirements can reduce technical barriers while leaving reconstruction of differentiated functionality dependent on additional conditions. Dependence beyond one instrument's reach is not, by itself, evidence of regulatory failure. The legal design question is whether responsibility for the remaining dependence is allocated to actors and instruments capable of governing it and whether residual continuity risk is addressed elsewhere. Section III applies this framework to EU financial law, examining cloud arrangements in which the Data Act and DORA govern the same exit through different actors and legal techniques.

III. Cloud exit in EU financial law

EU financial law makes the allocation of responsibility for cloud exit and continuity especially clear. Cloud reliance is governed within digital operational resilience, which places ICT third-party risk-management obligations on financial entities and establishes oversight of critical ICT third-party providers. The Data Act adds a horizontal layer of switching duties imposed directly on providers of data processing services. Where both regimes apply to a cloud arrangement, the same exit is governed through different actors

[28] Hayward and others, *supra,* note 24, 4–8.

[29] SWD (2020) 198 final, 18–19.

[30] Financial Stability Board, *supra,* note 12, 3–4. The FSB also emphasises that cloud services can improve institution-level resilience and states that it had not identified an immediate financial-stability risk from cloud use at the time of the report.

[31] DORA, Art. 28(8); Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers [2024] OJ L 2024/1773, Art. 10.

https://doi.org/10.1017/err.2026.10178

and legal techniques. This section first explains how DORA embeds exit within the financial entity's management of ICT third-party risk and continuity. It then examines the Data Act's provider-side switching duties and the legally protected process of departure they create, before turning to Article 30 and the allocation of responsibility where continuation depends on reconstruction in another environment.

1. Exit within digital operational resilience

DORA situates cloud dependence within digital operational resilience. Its recitals treat ICT third-party dependence as a source of concentration risk with possible systemic effects and describe the Union financial ecosystem as intrinsically dependent on ICT services, including cloud computing, software solutions and data-related services.[32] The operative text defines ICT concentration risk by reference to dependence on one or more critical ICT third-party providers whose unavailability, failure or other deficiency may endanger critical or important functions or the financial stability of the Union as a whole.[33] European Central Bank (ECB) outsourcing data give this concern empirical weight: nearly all banks in its 2024 analysis had contracts for cloud-based critical functions, and on average they spent 13.5% more on cloud outsourcing than reported in the 2023 analysis.[34] For the cloud-exit problem examined here, exit forms part of the entity's responsibility to keep dependence on an ICT provider compatible with continuity of the regulated function when the arrangement has to be changed, replaced or brought back in-house.[35]

DORA embeds exit within *ex ante* ICT third-party risk management. Financial entities must manage ICT third-party risk within their ICT risk-management framework, maintain a register of contractual arrangements with ICT third-party providers and assess ICT concentration risk before entering new arrangements.[36] For ICT services supporting critical or important functions, they must adopt exit strategies, take account of provider-level risks and ensure that exit can occur without undue disruption to business activities or adverse effects on compliance, continuity and quality of service.[37] Article 30 of DORA gives this preparedness contractual form through requirements concerning access, recovery and return of data, cooperation with competent and resolution authorities, termination rights, notice periods and transition to another provider or to in-house arrangements.[38] Exit is thus incorporated into resilience planning before disruption occurs, requiring the entity to prepare both for termination of the relationship and protection of the supported function through the transition.

The delegated framework gives exit planning greater specificity. Commission Delegated Regulation 2024/1773 requires a documented exit plan for each arrangement supporting critical or important functions and requires the plan to be realistic, feasible and based on plausible scenarios and reasonable assumptions.[39] These requirements connect

[32] DORA, recitals 63, 67 and 79 and Art. 3(1). DORA defines digital operational resilience by reference to a financial entity's capacity to maintain operational integrity and reliability through the ICT capabilities needed to address security and support the continued provision and quality of financial services, including through disruptions.

[33] DORA, Art. 3(29). See also Art. 3(22), which defines a "critical or important function" by reference to the consequences that disruption or defective performance would have for the financial entity's performance, continuity of services and activities, or continuing compliance with financial-services law.

[34] ECB Banking Supervision, "Outsourcing Trends in the Banking Sector" (Supervision Newsletter, 19 February 2025), sections "Cloud outsourcing" and "Substitutability and reintegration" <https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2025/html/ssm.nl250219_2.en.html>(last accessed 14 October 2026).

[35] DORA, Arts. 28(1) and (8).

[36] DORA, Arts. 28(1), 28(3), 28(4)(c) and 29(1).

[37] DORA, Art. 28(8).

[38] DORA, Arts. 30(2)(d), 30(2)(g), 30(2)(h) and 30(3)(f).

[39] Commission Delegated Regulation (EU) 2024/1773, Art. 10.

https://doi.org/10.1017/err.2026.10178

documentary preparedness to the circumstances in which exit would actually occur and to the assumptions on which continuity through transition depends.

The reporting framework brings substitutability and migration difficulty into the supervisory record. DORA's register templates require information on substitutability, identified alternatives, exit plans, reintegration and discontinuation impact, and record reasons for limited substitutability including proprietary technology and difficulties in migrating data and workloads.[40] ECB Banking Supervision reported in February 2025 that 82% of critical functions outsourced to external providers were considered difficult or impossible to substitute and, of those, 95% were difficult or impossible to reintegrate.[41] These figures leave the causes of migration difficulty unresolved while establishing substitutability and reintegration as part of the supervisory context in which DORA's exit requirements operate.

DORA also reaches provider-side risk through its oversight framework for critical ICT third-party providers.[42] Each designated critical provider is assigned a Lead Overseer from among the European Supervisory Authorities. The Lead Overseer assesses the provider's ICT-risk arrangements, expressly including mechanisms for data portability, application portability and interoperability, and has investigative and recommendation powers.[43] Provider-side risk can be addressed through oversight while responsibility for managing ICT third-party dependence and continuity risk remains with the regulated entity. The Data Act adds the distinct direct switching obligations imposed on providers considered next.

2. *Provider-side duties for cloud switching*

The Data Act establishes a horizontal layer of switching duties imposed directly on providers of data processing services.[44] Where a financial entity uses cloud services covered by Chapter VI, those provider-side obligations operate alongside its existing responsibilities for exit preparedness and continuity.

Article 23 establishes the core provider-side switching obligation. Providers must take the measures laid down in Chapter VI to enable customers to switch to another provider, move to on-premises ICT infrastructure or, where relevant, use several providers in parallel. They must remove pre-commercial, commercial, technical, contractual and organisational obstacles that inhibit termination, conclusion of a new contract, porting of exportable data and digital assets, functional equivalence where applicable, and technically feasible unbundling.[45] Article 24 reinforces the source-side boundary by limiting the relevant responsibilities to services, contracts or commercial practices provided by the source provider.[46] Article 23 gives switching legal protection beyond termination by constraining the provider's ability to use the existing contractual, organisational or technical relationship to obstruct it.

[40] Commission Implementing Regulation (EU) 2024/2956 of 29 November 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 with regard to standard templates for the register of information [2024] OJ L 2024/2956, annex I, template B_07.01.

[41] ECB Banking Supervision, "Outsourcing Trends in the Banking Sector," *supra,* note 34, section "Substitutability and reintegration."

[42] DORA, Arts. 31–5; Commission Delegated Regulation (EU) 2024/1502 of 22 February 2024 supplementing Regulation (EU) 2022/2554 by specifying the criteria for the designation of ICT third-party service providers as critical for financial entities [2024] OJ L 2024/1502; European Supervisory Authorities, "List of Designated Critical ICT Third-Party Service Providers at Union Level" (18 November 2025) <https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital> (last accessed 14 October 2026).

[43] DORA, Arts. 31(1)(b), 33(1)–(3), especially Art. 33(3)(f), and 35(1)(b) and (d).

[44] Data Act, Ch. VI, especially Arts. 23–30. See also Arts. 1(1)(d), 1(2)(e) and 2(8).

[45] Data Act, Art. 23.

[46] Data Act, Art. 24.

https://doi.org/10.1017/err.2026.10178

The surrounding provisions turn the entitlement into a regulated switching process. Article 25 requires contractual terms addressing the right to switch, transitional periods, notice, reasonable assistance, business continuity and security during transition, information on known continuity risks, support for the customer's exit strategy and the categories of data and digital assets that can be ported. Article 26 requires disclosure of available procedures, methods, formats, restrictions, technical limitations and relevant standards or open interoperability specifications. Article 27 requires all parties involved, including the destination provider, to cooperate in good faith, enable timely data transfer and maintain continuity of the data processing service. Article 29 provides for the gradual withdrawal of switching charges.[47] These provisions address practical sources of provider-created friction, including restrictive terms, opacity, delay, unsupported transfer, disruption and exit costs.

Articles 25 and 27 protect continuity during the switching process. Destination-side reconstruction raises a separate question of whether the service can operate in the new environment after switching. Article 30 addresses the technical conditions of the post-switching service separately.[48] Legal protection against disruption during switching leaves the level of functionality achievable in the new environment to those separate rules.

The interaction of the two regimes places departure within a legal framework combining entity-side continuity preparation with provider-side switching obligations. By the time the technical conditions of migration are reached, prior planning, mandatory contractual terms, transition support, switching charge discipline and supervision already govern the exit process. Article 30 then specifies how far provider-side duties reach the service's operation after switching, making the distinction between protected departure and service reconstruction legally decisive.

3. *Architecture and residual cloud migration risk*

Article 30 is where instrument reach becomes decisive for the technical conditions of migration. The legal framework is strong at the point of exit, but the obligations governing post-switching outcomes differ by service type. For services concerning scalable and elastic computing resources limited to infrastructural elements, the provider must take all reasonable measures in its power to facilitate functional equivalence after switching.[49] For other data processing services, Article 30 proceeds through open interfaces, compatibility with common specifications or harmonised standards following publication of the relevant references, and export of exportable data where those standards or specifications have not yet been published.[50] Article 31 further qualifies this architecture for certain custom-built services not offered at broad commercial scale, for which Article 30(1) and (3), among other switching obligations, do not apply; limited-period non-production services supplied for testing and evaluation fall outside Chapter VI altogether.[51] EU law directs its strongest generally applicable duty concerning the post-switching service outcome to services limited to infrastructural computing resources, while other services are governed through more conditional duties of interface access, exportability and standards-based compatibility.

[47] Data Act, Arts. 25–7 and 29. Art. 25(2)(a) requires reasonable assistance, due care to maintain business continuity, information on known continuity risks and maintenance of a high level of security during switching; Art. 25(2)(b) requires support for the customer's exit strategy; Art. 27 imposes a good-faith cooperation obligation on all parties involved; Art. 29 provides for the gradual withdrawal of switching charges.

[48] Data Act, Arts. 25(2)(a)(ii)–(iv), 27 and 30; see also recital 97.

[49] Data Act, Art. 30(1). Article 2(37) defines functional equivalence by reference to re-establishing, on the basis of the customer's exportable data and digital assets, a minimum level of functionality in a new data processing service of the same service type, with comparable outcomes for shared features. See also recitals 86 and 92.

[50] Data Act, Arts. 30(2)–(5).

[51] Data Act, Art. 31(1)–(2). See also recital 98.

https://doi.org/10.1017/err.2026.10178

Functional equivalence is distinctive because it reaches beyond handover to operation of the service after switching. The duty is nevertheless bounded. It applies only to infrastructure-type services, requires reasonable measures within the source provider's power and extends only to features offered independently by both source and destination services.[52] The Data Act also distributes responsibility across the switching process. The source provider is responsible for extracting data in a machine-readable format, while uploading them into the new environment falls to the customer and destination provider unless a separate transition service has been obtained. The destination environment lies outside the source provider's access and insight, and recital 92 confines its obligation to measures short of rebuilding the service there.[53] Responsibility for the migration outcome is distributed across the source provider, customer and destination provider.

For other data processing services within Chapter VI, providers must make open interfaces available free of charge, including sufficient information to enable software to communicate with the service for data portability and interoperability.[54] Subject to Article 31(1), Article 30(3) also requires standards-based compatibility once the relevant references become applicable.[55] Pending publication of relevant references for services of the same service type, the provider must, at the customer's request, export all exportable data in a structured, commonly used and machine-readable format.[56] These significant technical duties govern interface access, compatibility and exportability while leaving general reconstruction of the service in the destination environment outside their scope.

The difference between these regimes is not, by itself, evidence of defective legal design. A broader obligation requiring a particular post-switching outcome becomes harder to justify where successful migration depends on conditions outside the source provider's control. The Data Act recognises those limits directly. Functional equivalence does not require reconstruction in another provider's infrastructure. Article 30(6) further limits provider responsibility by excluding requirements to develop new technologies or services, transfer protected digital assets or compromise security and service integrity.[57] Its interoperability framework likewise requires standards to accommodate technical advances, new functions and innovation and to preserve security and integrity.[58] Extending an obligation to secure a comparable post-switching outcome across highly differentiated environments could make the source provider responsible for reconstruction that also depends on the destination service, customer architecture and functionality outside its control. The differentiated regime consequently has a defensible regulatory rationale. The optimality of each boundary drawn by Article 30 remains open. Proportionality must therefore assess both the dependence reduced by stronger portability and the burdens created by extending provider responsibility.[59]

The rationale leaves the migration problem in place. The same characteristics that make migration harder can also make a source-provider obligation to guarantee

[52] Data Act, Art. 30(1); recitals 86 and 92.

[53] Data Act, recitals 85 and 92. Recital 85 distinguishes responsibility for extraction by the source provider from uploading by the customer and destination provider, absent a separate professional transition service.

[54] Data Act, Art. 30(2).

[55] Data Act, Arts. 30(3), 31(1) and 35(8).

[56] Data Act, Arts. 2(38) and 30(5). "Exportable data" encompasses input and output data, including metadata, directly or indirectly generated or cogenerated through the customer's use of the service, subject to the exclusions in Art. 2(38) for protected provider or third-party assets and data.

[57] Data Act, recital 92 and Art. 30(6).

[58] Data Act, Art. 35(1)(d)–(e).

[59] See Commission, "Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)" COM (2025) 837 final, recitals 17–18 and Art. 1(15), proposing lighter Ch. VI treatment for certain non-infrastructure services. The proposal provides a contemporary example of the same burden-sensitive regulatory logic.

https://doi.org/10.1017/err.2026.10178

reconstruction harder to formulate. Infrastructure services can themselves create lock-in through configuration, cost, skills, proprietary interfaces and incompatible environments.[60] The problem becomes especially acute where cloud use extends into managed, customised, software-mediated or provider-specific services, since migration may require application adaptation, reconfiguration, replacement of provider-specific functionality and operational work in the destination environment.[61] The legal boundary between infrastructural and higher-layer services is also imperfect and may diverge from the degree of migration difficulty.[62] Article 30 bounds source-provider responsibility as reconstruction becomes increasingly dependent on other actors and technical conditions.

The Article 35(8) repository illustrates how this conditionality arises in practice. As of October 2026, no published Article 35(8) repository references for interoperability of data processing services had been identified in the official EU sources reviewed. The European Commission's February 2026 interoperability study was presented as assisting establishment of the repository and preparation of the first batch of open specifications and harmonised standards. The 2026 annual standardisation work programme likewise treated interoperability for data processing services as ongoing work.[63] Article 30(5) retained practical importance by securing exportability in a usable format pending operation of the repository-triggered compatibility obligation. This is a contingent feature of the present regime rather than the basis of the wider argument. Once relevant standards become applicable, standards-based compatibility can reduce migration barriers while remaining short of a general entitlement to reconstruction of provider-specific functionality.

Supervisory evidence indicates what remains beyond transfer and interface access. The ECB's cloud outsourcing guide treats exit as an explicitly technical exercise, identifying granular technical planning, time and cost, required tasks and skills, application complexity and periodic testing among relevant considerations. It distinguishes relatively portable infrastructure-as-a-service (IaaS) technologies such as virtual machines and container-based applications from platform-as-a-service (PaaS) and software-as-a-service (SaaS), whose portability depends on the specific solutions used, and warns that some service configurations may prevent resumption by another provider or by the supervised entity after termination.[64] The operational problem can persist even where the source provider has complied with the legal duties governing departure and transfer.

The Dutch Authority for the Financial Markets (AFM) and De Nederlandsche Bank (DNB) identify how deeper integration intensifies the same migration dependence. Their joint report describes technology vendors as moving higher up the technology stack and becoming more deeply embedded in the operational core of financial institutions. Migration becomes harder as applications and data are tailored to a particular provider ecosystem, and extensive use of a provider's PaaS and SaaS suite increasingly constrains workload

[60] Jamshidi, Ahmad and Pahl, *supra,* note 19; Opara-Martins, Sahandi and Tian, *supra,* note 19.

[61] Andrikopoulos and others, *supra,* note 19; Gholami and others, *supra,* note 19.

[62] Ennis and Evans, *supra,* note 7. Their criticism that the line between infrastructural and higher layer services is increasingly artificial remains relevant to the classification problem. The narrower point here is that the legal boundary remains operative even though service type is an imperfect proxy for migration difficulty.

[63] Commission, "Results of the Study on Interoperability of Data Processing Services" (Shaping Europe's Digital Future, 23 February 2026) <https://digital-strategy.ec.europa.eu/en/library/results-study-interoperability-data-processing-services>(last accessed 14 October 2026); Commission Notice, "The 2026 Annual Union Work Programme for European Standardisation" [2026] OJ C 2026/1695. The official sources reviewed for this article did not identify published art 35(8) repository references for interoperability of data processing services as of October 2026.

[64] ECB Banking Supervision, Guide on Outsourcing Cloud Services to Cloud Service Providers (European Central Bank 2025), sections 2.2 and 2.4.2–2.4.3 <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202507.en.pdf>(last accessed 14 October 2026). The Guide expresses ECB supervisory expectations and good practices rather than creating new legally binding requirements.

https://doi.org/10.1017/err.2026.10178

mobility.[65] These findings locate the residual dependence in architecture, provider-specific functionality, customer capability and reconstruction in the destination environment.

DORA carries this remaining continuity problem through the entity-side resilience framework established above. For ICT services supporting critical or important functions, financial entities must be able to exit without detriment to continuity, identify alternatives, develop transition arrangements and sufficiently test and review their exit plans; the delegated framework requires those plans to be realistic and feasible.[66] DORA also recognises that substitutability may itself be constrained by limited alternatives, technical complexity, proprietary technology and migration difficulty. Critical-provider oversight can examine portability and interoperability mechanisms.[67]

The legal picture is more precise than a simple shortfall in portability. The Data Act bounds the source provider's responsibility for the destination outcome; DORA carries the remaining continuity problem through obligations imposed on the financial entity. The vulnerability concerns whether those entity-side arrangements provide a workable basis for migration that preserves the regulated function.

IV. Exit, migration and the limits of cloud risk regulation

A binding right to exit a cloud provider can leave a customer unable to migrate because the legal obligations governing departure do not, by themselves, secure the conditions necessary to reconstitute and continue the service elsewhere. The Data Act makes switching legally enforceable by regulating contractual, commercial and technical obstacles and requiring provider cooperation. Its technical duties, however, do not extend uniformly to the reconstruction of services in another environment. Article 30 requires reasonable measures towards functional equivalence for services limited to infrastructural elements, while other services are governed through obligations concerning interfaces, exportability and, where applicable, standards-based compatibility. The departing provider is not required to rebuild applications or reproduce provider-specific functionality in the destination environment. Successful migration may consequently depend on the customer's architecture, the capabilities of the receiving provider and technical work beyond the source provider's control. In financial services, DORA addresses this remaining dependence through the financial entity's responsibility for preserving the continuity of critical or important functions.[68]

This distribution of responsibility reflects a defensible regulatory choice. Extending functional equivalence across differentiated PaaS and SaaS environments would make the departing provider responsible for outcomes partly determined by another provider's technology, the customer's applications and the configuration of the destination service. Such an obligation would be difficult to specify and could impose disproportionate burdens on differentiated cloud services.[69] The limits placed on provider-side duties therefore have a rationale independent of the migration difficulties they leave unresolved. Instrument reach captures this distinction by directing attention to the actor, dependency and outcome governed by a legal obligation. A duty can be effective within its defined scope while important conditions of operational continuity remain elsewhere. The difficulty is particularly consequential where the customer must adapt applications, replace provider-

[65] Dutch Authority for the Financial Markets and De Nederlandsche Bank, "Digital Dependence of the Financial Sector: Risks, Resilience and European Autonomy" (2025) 10, 14, 19 <https://www.afm.nl/~/profmedia/files/rapporten/2025/digital-dependence-of-the-financial-sector.pdf>(last accessed 14 October 2026).

[66] DORA, Art. 28(8); Commission Delegated Regulation (EU) 2024/1773, Art. 10.

[67] DORA, Arts. 31(2)(d), 33(3)(f) and 35(1)(d).

[68] DORA, Arts. 28–30; Data Act, Arts. 23–30 and recitals 85 and 92.

[69] Data Act, recital 92 and Arts. 30(6) and 35(1)(d)–(e).

https://doi.org/10.1017/err.2026.10178

specific functions or reconstruct security arrangements before the service can operate in another environment.

For financial entities, DORA provides the legal basis for governing those remaining conditions. Its existing requirements already connect exit from ICT providers supporting critical or important functions to continuity, realistic and feasible planning, and sufficient testing.[70] Reading these obligations alongside the Data Act clarifies what compliance should substantiate when the departing provider has fulfilled its switching responsibilities. A financial entity may possess enforceable termination rights, receive the required switching assistance and identify an alternative provider while still lacking a workable means of continuing the regulated function after migration. DORA's exit-planning obligations should therefore substantiate a credible, feasible and sufficiently tested path for reconstituting and continuing that function. This interpretation develops the evidentiary significance of existing resilience requirements rather than creating a new obligation to guarantee migration success or demanding technical identity between the source and destination services.

The practical significance of this interpretation lies in the assumptions on which exit plans depend. A plan may identify an alternative provider and contain the prescribed documentary elements while leaving substantial uncertainty about the operational work required to move. Its credibility depends on whether the contemplated exit scenario can support continuity in practice. Supervisory assessment should accordingly examine the proposed destination, the applications and configurations requiring adaptation, the provider-specific functions needing replacement, and any dependencies that would persist after departure. The assessment also concerns the availability of expertise, the time required for transition, the preservation of security and regulatory compliance, and the extent to which critical migration steps and service resumption have been tested.[71] These questions connect DORA's requirements of feasibility and testing to the actual technical and organisational conditions of migration, rather than treating the existence of an exit plan as sufficient evidence of operational preparedness.

The supervisory record shows why such scrutiny matters. DORA's register already captures information on available alternatives, proprietary technology, discontinuation impact, exit planning and difficulties in migrating data and workloads.[72] ECB Banking Supervision reported that 82% of critical functions outsourced to external providers were considered difficult or impossible to substitute and that 95% of those functions were difficult or impossible to reintegrate.[73] AFM and DNB likewise identify growing dependence where financial institutions become embedded in provider-specific ecosystems and higher-layer cloud services.[74] These findings do not establish how frequently migration fails following legally compliant switching. They do, however, reveal the practical limits of treating the identification of an alternative as evidence that the regulated function can be continued there. The information already collected through supervision provides a starting point for examining those limits, although the credibility of a particular migration path ultimately depends on the technical assumptions and testing underpinning the entity's exit arrangements.

The distinction acquires further significance as EU cloud policy moves beyond facilitating exit towards expanding alternative capacity and, in certain circumstances, requiring

[70] DORA, Art. 28(8); Commission Delegated Regulation (EU) 2024/1773, Art. 10.

[71] ECB Banking Supervision, *Guide on Outsourcing Cloud Services to Cloud Service Providers*, *supra,* note 64, sections 2.4.2–2.4.3. The ECB Guide identifies, among other matters, technical exit planning, migration time and cost, tasks and skills, application complexity and periodic testing of critical migration steps.

[72] Commission Implementing Regulation (EU) 2024/2956, annex I, template B_07.01.

[73] ECB Banking Supervision, "Outsourcing Trends in the Banking Sector," *supra,* note 34, section "Substitutability and reintegration."

[74] Dutch Authority for the Financial Markets and De Nederlandsche Bank, *supra,* note 65, 10, 14–15, 19–20.

https://doi.org/10.1017/err.2026.10178

migration. The European Commission's June 2026 proposal for a Cloud and AI Development Act (CADA) seeks to strengthen European cloud and AI capacity and address cloud sovereignty risks.[75] Under proposed Article 29, sovereignty-risk assessments concerning public sector cloud use may require migration to another provider. Article 29(6) would require such movement within a reasonable transition period of no more than twelve months, taking account of technical feasibility, service continuity and applicable data-portability requirements.[76] The proposal brings into view three distinct conditions of movement: the availability of an alternative destination, the legal requirement to move and the operational capacity to continue after moving. Greater domestic capacity may expand the destination set, and a migration requirement may establish when departure must occur. Neither determines whether applications can be adapted, provider-specific functions replaced or the service securely resumed within the prescribed period. The proposed deadline makes the feasibility of those tasks a particularly consequential part of the migration decision.

The broader regulatory problem therefore concerns how instruments governing different dimensions of dependence relate to the operational outcomes they seek to secure. Capacity-building can enlarge the range of alternatives, switching rules can make departure enforceable, sovereignty requirements can mandate movement, and resilience law can require preparation for continuity. Each addresses a distinct condition of migration, and each may be justified on its own terms. Their interaction nevertheless matters because the operational outcome depends on conditions that no single instrument necessarily governs in full. The contribution of instrument reach is to distinguish what compliance with a particular duty establishes from what remains to be demonstrated through other responsibilities. In EU financial law, this distinction connects the Data Act's bounded provider-side obligations with DORA's requirement for credible continuity preparedness. More generally, it reveals a vulnerability in regulatory architectures that distribute responsibility for a shared operational outcome across different instruments. That vulnerability arises when success under one instrument is treated as evidence of an outcome beyond its reach.

Data availability statement. None.

Acknowledgments. The author wishes to thank the reviewers and editorial team of the European Journal of Risk Regulation (EJRR) for their constructive feedback and guidance, which helped strengthen the article's argument. Any remaining shortcomings are solely the author's responsibility.

Financial support. This work has received funding from the European Research Council (ERC) under the European Union's Horizon Europe research and innovation programme (Grant Agreement No. 101116328). Open access funding was provided by Vrije Universiteit Brussel (VUB).

Competing interests. None.

[75] Commission, "Proposal for a Regulation of the European Parliament and of the Council Establishing a Framework of Measures for Strengthening Europe's Cloud and AI Ecosystem (Cloud and AI Development Act)" COM (2026) 502 final (procedure 2026/0138(COD)); European Parliament, Legislative Observatory, "Cloud and AI Development Act (2026/0138(COD))" <https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2026%2F0138%28COD%29>(last accessed 14 October 2026) (procedure awaiting committee decision).

[76] CADA proposal, Art. 29(6). See also Bundesverband der Deutschen Industrie, "Cloud and AI Development Act: Evaluation of the European Commission's Regulatory Proposal" (Position Paper, 5 October 2026) 16 <https://bdi.eu/media/pages/publications/cloud-und-ai-development-act/c522b3c462-1791361190/2026-10-05-bdi-position-cada.pdf>(last accessed 14 October 2026), questioning the feasibility of the proposed twelve-month ceiling for complex migrations, particularly SaaS, and recommending at least twenty-four months or case-specific extensions where technical complexity, continuity requirements or contractual dependencies warrant them.

Cite this article: M Javadi, "Exit without Migration: Cloud Switching and Operational Continuity in EU Law". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2026.10178

https://doi.org/10.1017/err.2026.10178