Implementing the DMA

De Streel, Alexandre; Bourreau, Marc; Feasey, Richard; Fletcher, Amelia; Kraemer, Jan; Monti, Giorgio

Publication date:
2024

Document Version
Publisher's PDF, also known as Version of record

cerre Centre on Regulation in Europe

IMPLEMENTING THE DMA: SUBSTANTIVE AND PROCEDURAL PRINCIPLES

ALEXANDRE DE STREEL (COORD)
MARC BOURREAU
RICHARD FEASEY
AMELIA FLETCHER
JAN KRAEMER
GIORGIO MONTI

January 2024

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Amazon, Apple, Booking.com, DuckDuckGo, Epic Games, Google, Aspiegel, MFE-MediaForEurope, Meta, Microsoft, Mozilla Corporation, and Qualcomm. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

1. its original, multidisciplinary and cross-sector approach;
2. the widely acknowledged academic credentials and policy experience of its team and associated staff members;
3. its scientific independence and impartiality;
4. the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

ABOUT THE AUTHORS

Marc Bourreau is an Academic Co-Director at CERRE and Professor of Economics at Télécom Paris (Institut Polytechnique de Paris). He is affiliated with the interdisciplinary institute for innovation (i3) for his research. His research focuses on competition policy and regulation, digital markets, and telecommunications. Marc holds a Ph.D. in Economics from the University of Paris Panthéon Assas.

Richard Feasey is a CERRE Senior Advisor, an Inquiry Chair at the UK's Competition and Markets Authority and Member of the National Infrastructure Commission for Wales. He lectures at University College and Kings College London and the Judge Business School. He has previously been an adviser to the UK Payments Systems Regulator, the House of Lords EU Sub-Committee and to various international legal and economic advisory firms. He was Director of Public Policy for Vodafone plc between 2001 and 2013.

Amelia Fletcher CBE is a CERRE Research Fellow, and a Professor of Competition Policy at the Centre for Competition Policy, University of East Anglia. She is also a Non-Executive Director at the UK Competition and Markets Authority, and a member of the Enforcement Decision Panel at Ofgem (she is a Non-executive Director at the U.K. CMA but the views expressed here are her own)

Jan Krämer is an Academic Co-Director at CERRE and a Professor at the University of Passau, Germany, where he holds the chair of Internet & Telecommunications Business. Previously, he headed a research group on telecommunications markets at the Karlsruhe Institute of Technology (KIT), where he also obtained a diploma degree in Business and Economics Engineering with a focus on computer science, telematics and operations research, and a Ph.D. in Economics, both with distinction.

Giorgio Monti is a CERRE Research Fellow and Professor of Competition Law at Tilburg Law School. He began his career in the UK (Leicester 1993-2001 and London School of Economics (2001-2010) before taking up the Chair in competition law at the European University Institute in Florence, Italy (2010-2019). While at the EUI he helped establish the Florence Competition Program which carries out research and training for judges and executives. He also served as Head of the Law Department at the EUI.

Alexandre de Streel is the Academic Director of the digital research programme at CERRE and Professor of European law at the University of Namur where he chairs the Namur Digital Institute (NADI). Alexandre is also visiting professor at the College of Europe (Bruges) and SciencesPo Paris. Besides, he chairs the expert group on the online platform economy advising the European Commission and is a part-time judge at the Belgian Competition Authority. His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence.

Previously, Alexandre held visiting positions at New York University Law School, European University Institute in Florence, Barcelona Graduate School of Economics and University of Louvain. He also worked for the Belgian Deputy Prime Minister, the Belgian Permanent Representation to the European Union and the European Commission.

FOREWORD

In the dynamic landscape of EU digital platforms regulation, we are at a focal point of discussions shaping the future of implementation of the Digital Markets Act – arguably one of the most important pieces of legislation of the current times' digital policy sphere.

With the DMA aiming for contestability and fairness in digital markets, designated gatekeeper platforms are set to unveil their compliance plans on March 2024. The European Commission, in its unique role as an enforcer, will lead the work of determining non-compliance and ensure that the DMA fulfils its ambitious goals.

However, the success of implementation will depend on the principles on which the new law will be applied. This CERRE report recommends that the DMA implementation process should be guided by the substantive principles of effectiveness, proportionality, non-discrimination, legal predictability, and consistency with other EU laws. Furthermore, the Commission will have to approach enforcement taking into account the procedural principles of responsive regulation and participation, due process, and ex ante and ex post evaluation. The report then applies those principles to series of specific DMA obligations: choice architecture, horizontal and vertical interoperability and data related obligations.

It is also essential to agree on how the Commission, gatekeepers, and third parties will engage with each other. The DMA provides a model of compliance which is not based solely on deterrence; instead, the gatekeepers are encouraged to and will comply by engaging co-operatively with the Commission and third parties. However, it is still up for question how this principle will be applied, what it expects from the stakeholders, and how the Commission itself will exercise its deterring powers to enforce compliance.

On top of it all, this CERRE DMA edition is also proposing a set of quantitative measurement indicators, so-called output indicators, each relating to a particular obligation or set of obligations, in order to better understand the impact of obligations on the relations between gatekeepers and third parties. These quantitative indicators will not represent specific targets or thresholds against which compliance should be assessed. They will neither attempt to measure the effect of changes in conduct on market outcomes for users nor, more generally, competition. These quantitative measures will be added to other evidence, such as complaints or qualitative representations from affected parties, including gatekeepers, which the Commission will consider in its compliance assessments.

This report was written in the framework of a 8-months-long, multi-stakeholder CERRE initiative entitled the 'DMA Compliance Forum' that created a neutral and trusted platform and facilitated dialogue among CERRE members and academics to contribute to the effective and proportionate enforcement of the regulation.

Bruno Liebhaberg, CERRE Director General

cerre Centre on Regulation in Europe

DMA IMPLEMENTATION PRINCIPLES

ALEXANDRE DE STREEL

1. THE FEATURES OF THE DMA

The DMA has **two main objectives**: to ensure contestability (i.e., the reduction of entry barriers) and to ensure fairness (i.e., a balance between the rights and obligations of the gatekeepers and their business users) of EU digital markets.[1] In turn, these objectives should lead to more innovation and choice for end-users.[2]

To achieve those objectives, the DMA imposes **a series of different types of obligations (and therefore different degrees of difficulty in enforcing them).** Some are (i) transparency obligations, in particular regarding online advertisement prices and performance, (ii) others consist of prohibitions which may be contractual and/or technical, and (iii) others consist of obligations to provide access to platforms (vertical or horizontal interoperability) or to data (portability or data sharing).[3]

Some access obligations will require changes in the products and services offered by the regulated gatekeepers. On the one hand, gatekeepers must design new interfaces and architectures to propose and manage more choices for the end users and consent mechanisms where personal data are involved. On the other hand, gatekeepers must also develop new technical tools to enable smooth access to their platforms for business users. These new choice architectures and technical tools for access and interoperability, and more fundamentally the logic of openness, should apply to new products but also to existing ones, leading to the re-engineering of some existing products.

The DMA obligations and the resulting changes in product design (and possibly in business models) are **particularly difficult to enforce,** as some of the biggest companies in the world are subject to them and enforcement may in some cases carry an important cost for these companies. Moreover, intervention needs to be swift and effective, since digital markets can easily tip, a reversal of which may be difficult to achieve.

To reduce these enforcement difficulties, the **DMA is an *ex-ante* legal tool whereby compliance must be demonstrated by the regulated gatekeepers**. Thus, compared to *ex post* competition law, the DMA shifts the burden of proof from the Commission (to show a violation of a competition law prohibition) to the gatekeeper (to show compliance with prohibitions and obligations).[4] This should ease and accelerate enforcement. However, if the Commission wants to condemn a gatekeeper for non or insufficient compliance, it remains subject to the burden of proving that the compliance measures adopted by the gatekeeper are insufficient to meet the obligations of the DMA. Hence, the shift in the burden of proof is obviously not complete.

To ease enforcement, the legislator has also granted **important procedural discretionary powers to the Commission**. For instance, the Commission may or may not take a complaint from a business user,

[1] DMA, Art. 1 (1).

[2] These objectives are implementing the European Declaration of 15 December 2022 on Digital Rights and Principles for the Digital Decade, OJ [2023] C 23/1, Points 10 and 11.

[3] DMA, Arts. 5-7.

[4] DMA, Rec. 5.

it may or may not specify an obligation, either upon the request of a gatekeeper or its own initiative, it may or may not adopt interpretative guidelines. This important procedural discretion is justified by the complexity of the enforcement process, the need to deter non-compliance or ineffective compliance, and the novelty of the law. However, the Commission must exercise its discretion in a non-discriminatory and impartial manner.

The DMA obligations will also be difficult to implement because they apply to digital ecosystems which are complex and constantly evolving, not always fully understood. Therefore, **the DMA obligations inevitably lead to a number of trade-offs**. In particular, there is a trade-off between platform openness and service security, privacy, or integrity. There is also a trade-off between contestability and user autonomy. These trade-offs are acknowledged in the DMA. Some of the connected balancing will have to be done in the implementation process by gatekeepers when adopting their compliance measures, then by the Commission or national Courts when assessing these measures and, ultimately, they will be adjudicated by the Court of Justice of the EU when ultimately interpreting of the DMA.

2. SUBSTANTIVE PRINCIPLES

The implementation of the DMA should respect several substantive principles, which are derived from the theory of good regulation[5] and which are, more or less explicitly, mentioned in the DMA. They are effectiveness, proportionality, non-discrimination, legal predictability, and consistency with other EU laws.

2.1. Effectiveness

Effectiveness is a key principle of the DMA and plays a role at various instances in its implementation.

First, the **gatekeeper must prove that their compliance measures are effective** in two ways: (i) in achieving the objectives of the DMA as a whole (general effectiveness) and (ii) in achieving the objectives of each obligation (specific effectiveness).[6]

- General effectiveness refers to the DMA's two overarching objectives of contestability and fairness. Contestability mostly relates to reducing strategic and some structural entry barriers, while fairness is an issue where the imbalance between gatekeeper and business user deprives the latter of adequate reward for its efforts. In the end, both objectives may be understood with reference to (long-term) competition in digital markets among the gatekeepers and between the gatekeepers and business users.
- Specific effectiveness relates to the objectives of each obligation which can be measured with quantitative metrics on the impact of obligations on relations between the gatekeeper and third parties.

Second, the **gatekeepers cannot circumvent the obligations** by engaging in conduct of a contractual, commercial, technical, or of any other nature that undermines effective compliance with the DMA obligations.[7]

Third, the **Commission may specify the obligations** contained in Articles 6 and 7 to ensure that measures adopted by the gatekeeper **achieve double effectiveness**.[8] If implementation shows that the initial specification does not lead to effectiveness, the Commission may then re-specify the obligations.[9]

[5] R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation: Theory, Strategy and Practice*, 2nd ed, 2012, Oxford University Press; Viscusi, Harrington and Shappington, *Economics of Regulation and Antitrust*, 5th ed, MIT Press, 2018. Also P. Larouche, Code of conduct & best practices for the setup, operations, and procedure of regulatory authorities, CERRE Report, May 2014.

[6] DMA, Art. 8 (1) and 13 (3).

[7] DMA, Art. 13(4).

[8] DMA, Art. 8(7).

[9] DMA, Art. 8(8).

Fourth, if the DMA obligations no longer effectively ensure contestability and fairness, because of the evolutions of technologies and markets, the **Commission may extend the scope of existing obligations in a delegated act**.[10] This aims to maintain the effectiveness of the obligations in rapidly evolving markets.

More generally, effectiveness is a key principle used by the Court of Justice to interpret EU law. Indeed, the Court relies on systemic and teleological interpretation of the law to ensure its effectiveness and does not limit itself to the literal interpretation.[11]

2.2. Proportionality

Proportionality is also a general principle of EU law which requires, according to the EU Treaties, that the content and form of the public intervention should not exceed what is necessary to achieve the objectives of such intervention.[12]

This important principle plays two main roles in the implementation of the DMA.

2.2.1. Proportionality of the compliance measures

First, the **measures adopted by the gatekeepers to comply with the DMA should not exceed what is necessary to achieve contestability and fairness in EU digital markets**. In proposing their compliance measures, gatekeepers have a natural incentive not to go further than what is necessary, and therefore the allocation of the burden of proof in the DMA contributes to the self-execution of the proportionality principle.

When the **Commission specifies the measures required to comply with an obligation**, it should ensure that those measures achieve the double effectiveness mentioned above but also that they are **proportionate in the specific circumstances pertaining to the gatekeeper and the relevant service**.[13] Thus, if multiple measures are equally effective, the Commission should choose the one which is the least intrusive for the gatekeepers.[14]

In doing so, the application of the proportionality principle also contributes to **avoiding or mitigating the risks of unintended consequences** of the DMA implementation, in particular, the reduction of innovation and consumer choice which are the ultimate objectives of the DMA.

2.2.2. Proportionality of the defences

Second, **when the gatekeeper relies on the service integrity, security, or privacy defence allowed in the DMA, it should do so in a proportionate manner**.[15] In this case, it is incumbent for the gatekeepers

[10] DMA, Art. 12.

[11] Such interpretative methods have been used by the Court of Justice since its very early case law, for instance in Case 26/62 *Van Gend en Loos* and in Case 6/64 *Costa v ENEL*.

[12] TEU, Art. 5(4).

[13] DMA, Art. 8(7).

[14] Specifically, the proportionality principle channels the economic analysis that normally underpins an efficiency defense in antitrust (butis not present in the DMA) into a narrower framework and it compels the defendant firm to work within the specific set of core goals of the DMA.

[15] DMA, Art. 6(3), 6(4), 6(7), 7(3) and 7(6).

to show that their measures are strictly necessary and proportionate, to protect the integrity, security, and privacy of their services. Thus, if different measures achieve the same degree of integrity, security, and privacy, the gatekeeper should choose the one which is the least detrimental to contestability and fairness.

In this case, the principle is probably not self-executing as the gatekeepers may not have an incentive to choose the measures which are the least detrimental to contestability and fairness. This is why the Commission should be strict in controlling the use of the defense in the process of assessing the legality of the compliance measures proposed by the gatekeepers or when it specifies the measures to be adopted by the gatekeepers.

In doing so, this **second type of application of the proportionality principle allows the enforcers of the law to balance the different trade-offs of the DMA mentioned above**. It also contributes to **consistency across different legislations** which compose the quickly expanding EU digital platforms acquis and is conducive to solving the tension between different laws with divergent objectives.

2.3. Non-discrimination

Contrary to effectiveness and proportionality, the principle of non-discrimination is not explicitly and directly mentioned in the DMA. However, it is a principle of good regulation and it underpins the contestability objective, as contestability aims to ensure equality of chance among business users and gatekeepers, a form of non-discrimination. It also underpins several DMA obligations, for instance, regarding choice architecture which should avoid discrimination that favours gatekeepers over challengers[16] or the implementation of interoperability obligations.[17]

While the DMA does not necessarily consider gatekeepers as public utilities which are obliged to deal with all users in a neutral way, the **principle of non-discrimination and absence of conflict of interest could play an important role in verifying compliance**. Indeed, a differentiation of treatment between the gatekeeper and third parties could be seen as a violation of the DMA obligations when it is unjustified.

The application of this principle also means there needs to be a **consistent application of the rules across gatekeepers** and that the Commission should ensure equal treatment among them.

2.4. Legal Predictability

Legal predictability is also a principle of good regulation, as it shapes the expectations and the incentives of the regulated firms (the gatekeepers) as well as the beneficiaries of the regulation (the business users or the gatekeepers entering other markets than those in their core realm of activities). While the Articles of the DMA do not mention legal certainty explicitly, several recitals refer to it.[18] This principle is particularly **important for gatekeepers which may have to significantly re-design**

[16] Issue paper Choice Architecture for End Users in the DMA, Section 3.3.

[17] Issue paper Horizontal and Vertical Interoperability in the DMA, Section 6.

[18] DMA, Rec. 20, 30, 73, 77, and 103.

their products and services, as well as for entrants which may invest a lot in innovative offerings made possible by the DMA in the course of DMA implementation.

To achieve this principle, the **Commission has several means to increase legal predictability** and clarifying the interpretation of some obligations with guidelines,[19] individual acts, or generally applicable implementing acts.[20]

However, there is an inevitable **tension between legal predictability and the legal flexibility** which is needed to adapt the regulation to the insight gained from past implementation [21] and to the evolution of technologies and markets. This is why the DMA provides for mechanisms in which the Commission can re-specify the measures needed to comply with regulatory obligations,[22] to extend the scope of existing obligations, or to propose the EU legislature to add or remove obligations.[23] In using those flexibility mechanisms, the Commission should nonetheless be predictable and show how the regulatory adaptations contribute to contestability and fairness as well as to the effectiveness of the rules.

2.5. Coherence with Other Laws

As several DMA prohibitions and obligations relate to rights and interests protected by other EU and national legislative instruments, it is important that the **DMA is implemented in way which is consistent with those other instruments**.

This is obviously the case with competition law, given the antitrust roots of the DMA. But this is also the case for data laws (in particular the GDPR, the Data Governance Act, and the Data Act) and cybersecurity laws (NIS Directive, Cybersecurity Act, etc.). It is **key that the new platform and data openness and variety in user choices created by the DMA does not undermine data privacy and security,** and ultimately the trust of the users in the (big and small) providers of digital services or, more generally, in the digital society overall. For this, the new privacy and security risks should be managed carefully by all stakeholders involved in the DMA implementation and users should be educated on the possibilities and risks associated with their new choices. This is why the DMA should be implemented in a manner consistent with EU laws which deal with those risks, in particular through a close dialogue between the authorities in charge of the different EU laws within the DMA High-level group.[24]

[19] DMA, Art. 47

[20] Resp. DMA, Art. 8(2) and 46(1b).

[21] In that regard the Recommendation of the OECD Council of 6 October 2021 for Agile Regulatory Governance to Harness Innovation, OECD/LEGAL/464 advises the regulators to move from a 'regulate and forget' approach to a 'learn and adapt' approach.

[22] DMA, Art. 8(9).

[23] Resp. DMA Art. 12 and 19.

[24] DMA, Art.40.

3. PROCEDURAL PRINCIPLES

Next to the substantive principles, the implementation of the DMA should also follow several procedural principles which are similarly derived from good regulatory practices in liberal democracies. Those principles are particularly important because on the one hand, the quality of the process will determine the outcome of the DMA and, on the other hand, the Commission – which is a political institution – enjoys important procedural discretion in implementing the DMA. The principles are: responsive regulation and participation, due process, and *ex ante* and *ex post* evaluation.

3.1. Responsive Regulation and Participation

While the DMA has no hierarchy of enforcement methods, an **approach based on responsive regulation should be deployed**.[25] This system relies on assuming that gatekeepers wish to comply and that third parties have a voice in shaping that compliance effort. It follows that the first stage is to persuade gatekeepers to comply via regulatory dialogue informed by the views of third parties. If this does not secure compliance, then enforcement can become progressively harsher until the gatekeeper responds to these signals and complies. This means that greater recourse is made to the supervisory measures in the DMA than to the punitive measures.

Participation relies on a **number of dialogues, the structure of which should be transparent and give incentives to all stakeholders to effectively increase contestability and fairness** in the EU digital markets. As explained in the companion paper on DMA Process and Compliance, three main dialogues are organised by the DMA:[26]

- First, *a dialogue between the gatekeepers and the Commission* which may be informal or formal in the context of a specification decision (Article 8) or a non-compliance decision (Article 29); such dialogue should be as transparent as possible (while respecting confidentiality of business secrets) and ensure an equal treatment among the different gatekeepers;
- Second, *a dialogue between the gatekeepers and the third parties* which is particularly important for the effectiveness of those DMA obligations which require new product designs in the form of new choice architectures and technical tools for access and interoperability; experience in other regulated sectors shows that such dialogue should be carefully structured and steered by the Commission; it should be based on coordination amongst business users before the dialogue with gatekeepers and the establishment of working groups on technical and non-technical issues to address operational and legal matters;

[25] Issue paper Process and Compliance, Section 2.

[26] Ibid, Section 3.

- Third, *a dialogue between the Commission and third parties* which may informally take place at any time, or more formally in the context of a specification decision or a non-compliance decision; such dialogue should ensure that third parties are heard when this is useful for the effectiveness of the implementation of the DMA and that the Commission can prioritise its resources to maximise such effectiveness.

4. EVALUATION OF COMPLIANCE MEASURES

(a) Ex ante evaluation

Before the gatekeeper decides on compliance measures and the Commission judges their legality, **experimental *ex ante* testing is useful. This testing can take three main forms**:[27]

- *Lab experiments* which involve participants being asked to make choices in a clear experimental context;
- *Field trials* (also known as A/B testing or randomised controlled trials/RCTs) which involve trialling different options with real end users, in real choice environments, who are unaware they are part of an experiment, and analysing their reaction;
- *End user surveys* which provide useful directional indicators of how end users may be expected to react to particular measures and can also be valuable for collecting qualitative information.

These different types of testing are complementary, as they may be done by different stakeholders (field trials are best done by gatekeepers, while business users could do lab experiments and user surveys) and give different results. Specifically, field trials involve real choices which is not the case in lab experiments.

The **gatekeepers should be incentivised to run field trials** before determining and reporting on their selected compliance measures, but only in a proportionate manner taking into account the costs of running those trials. The compliance report should contain an explanation of contractual and technical measures which were envisaged, which measures were finally adopted and why.[28] In addition, the Commission and business users may also wish to carry out their own *ex ante* testing, both to understand the likely impact of measures taken by the gatekeepers and more specifically to inform the Commission's oversight of the gatekeepers' own testing programmes.

[27] Issue paper Choice Architecture for End Users in the DMA, Section 4.2.

[28] Commission Template for Compliance Report, point 2.1.2. (i) (o).

(b) Ex post evaluation

As explained above, the gatekeeper has the burden to prove compliance and the compliance report is the key instrument to do so.[29]

The Commission should assess the legality of the selected compliance measures and when not satisfied, the Commission may open a dialogue with the gatekeeper or open a procedure for non-compliance. In that regard, **the output indicators delineated in a companion paper could help the Commission to focus its attention on where additional pieces of evidence may be required to judge DMA compliance; these indicators would not constitute direct evidence of (non) compliance**.[30] Thus, alongside other information submitted by the gatekeeper, third parties, or assembled by the Commission itself, output indicators would inform an overall assessment of whether the gatekeeper has complied with the relevant obligation, and in case of non-compliance, why this has occurred and what steps might be required to remedy any breach.

4.1. Due Process

Because the DMA obligations limit the freedom to conduct business guaranteed by the EU Charter on Fundamental Rights,[31] the **Commission should exercise its DMA implementing powers in full adherence to due process**. In that regard, the DMA contains several provisions, in particular on requests for information, the power to carry out interviews and take statements, powers to conduct inspections, the right to be heard and to access the file, and professional secrecy.[32]

The respect of those principles is particularly important because the Commission does not necessarily meet the independence requirements[33] that EU constitutional and secondary laws generally impose on national regulatory authorities.[34]

In the future, secondary legislation to codify procedures may be required to ensure fundamental rights protection and respect for the principles of good administration. As explained in the companion paper on DMA Process and Compliance, **best practice documents which accompany procedural rules can emerge** as they have in antitrust.[35]

[29] DMA Art. 8(1) and Compliance Report Template, Section 2.

[30] Issue paper Output indicators.

[31] EU Charter of Fundamental Rights, Art. 16.

[32] DMA, Arts. 21, 22, 23, 34, and 36 respectively.

[33] Speech Commissioner Reynders noting that: "(…) based on Article 8 of the Charter, the enforcer of data protection rules must be ensured by an independent authority. Therefore, the Commission could not have (this) enforcing powers."

[34] On the need of independence for good regulatory enforcement, see C. Decker, *Modern Economic Regulation: An Introduction to Theory and Practice*, Cambridge University Press, 2014, Ch. 7; P. Larouche, C. Hanretty, and A. Reindl, *Independence, Accountability and Perceived Quality of Regulators*, CERRE Report, 2012.

[35] Issue paper on DMA process and compliance, Section 6. https://competition-policy.ec.europa.eu/document/4dece098-82fb-4cdd-bd5c-1176c52e4531_en

4.2. Evaluation of the Effectiveness of the DMA

As is the case for most EU laws, the DMA requires the Commission to do an evaluation of the Regulation every three years to assess whether it achieves its objectives and gauge its impact on business users (in particular SMEs) and end-users.[36]

In its Better Regulation Guidelines, the Commission explains that: "**evaluation is an evidence-based assessment of the extent to which an intervention**: (i) is *effective* in fulfilling expectations and meeting its objectives; (ii) is *efficient* in terms of cost-effectiveness and proportionality of actual costs to benefits; (iii) is *relevant* to current and emerging needs; (iv) is *coherent* (internally and externally) with other EU interventions or international agreements; and (v) has *EU added value,* i.e. produces results beyond what would have been achieved by Member States acting alone."[37]

In the Better Regulation Guidelines, the Commission also notes that: "**a well-designed monitoring system should be governed by the following principles**: (i) *comprehensiveness,* i.e. covering all objectives of the intervention; (ii) *proportionality,* i.e. reflecting the costs of collecting information and the importance placed on different aspects of the intervention; (iii) *minimal overlap,* i.e. avoiding duplication and unnecessary data collection burdens by concentrating only on data gaps; these should be identified through a preliminary analysis of existing data collection; (iv) *timeliness,* not all evidence has to be collected at the same time but should be ready by the time of a planned evaluation; and (v) *accessibility,* in principle, all evidence should be made available to the public with clear information on their specificities and limitations, subject to confidentiality arrangements and rules on data protection."[38]

Therefore, the **Commission should already today prepare the evaluation by determining which indicators should be collected, by whom, and how**. In that regard, the output indicators proposed in a companion paper could inform an overall assessment of the effectiveness of the DMA measures. As the Commission is the enforcer of the DMA, it would be essential that the evaluation of the law is also done by an EU body which is fully independent from the Commission to alleviate any conflict of interest. One option would be the Court of Auditors whose tasks include "the submission of observations, particularly in the form of special reports, on specific questions and deliver opinions at the request of one of the other institutions of the Union" and which report to the EU legislature.[39]

[36] DMA, Art. 53.

[37] Commission Staff Working Document of 3 November 2021, Better Regulation Guidelines, SWD (2021) 305, p. 23.

[38] *Ibidem*, p. 40.

[39] TFEU, Art. 287(4). See https://www.eca.europa.eu/en/multiple-reports

1. EXECUTIVE SUMMARY

"Choice architecture" is a neutral term, which simply describes the way in which information and choices are presented to end users. This can include a wide variety of aspects relating to how choices are 'framed', including the number and ordering of options, whether any options are set as 'defaults' or made more prominent, the information provided at the time of choice, the information and screen provided prior to that choice (which can have 'priming' effects), the wording, the timing and frequency of choices, illustrations, and colours used, and so on.

Why does this matter? Because it is well understood that **these elements can steer user decision-making, subtly but powerfully**. Indeed, in some situations, this steering may be sufficiently strong that users are not even aware that they have a choice, a phenomenon which is sometimes referred to as 'dark patterns'.

In this report, we consider the importance of choice architecture design for effective compliance with the EU Digital Markets Act (DMA).[40]

First, we explain why choice architecture is important for such compliance. We then provide some overarching principles for effective compliance to guide the gatekeepers in ensuring that their choice architecture is designed in a compliant way.

Why is choice architecture important for compliance?

The DMA is heavily informed by a variety of highly prevalent and well-understood behavioural insights. For example:

- We know that end users are likely to choose the pre-installed browser or search engine and then stick with it, reflecting *default and status quo* effects respectively. To address this, Article 6(3) requires gatekeepers with proprietary browsers and/or search engines to ensure that consumers are given an active choice upfront. It also requires that gatekeepers make it easy to switch default settings more generally.

- We know that end users are most likely to choose the first or most prominent option in any ranking, reflecting *ranking* and *salience* effects respectively. This gives rise to a risk that gatekeepers could leverage their core market position into a related service by ranking the latter more highly and prominently than rival options. To address this, Article 6(5) prohibits gatekeepers from engaging in such self-preferencing in ranking.

[40] This issues paper builds on the 2022 CERRE paper "DMA switching tools and choice screens", which set out several issues of scope and implementation in relation to various elements of the DMA which involved issues of choice architecture. Published as a section in de Streel, A. et al (2023), "Effective and Proportionate Implementation of the DMA". Available at: https://cerre.eu/publications/effective-and-proportionate-implementation-of-the-dma-3/.

- A number of DMA provisions require that end users be able to carry out certain actions *easily*, reflecting the concern that users can be deterred by complexity.

These provisions all essentially relate to the gatekeepers' design of choice architecture. But the DMA goes further; it requires that gatekeepers not only comply with its provisions, but that it does so in a way that is effective in achieving the objectives of the DMA: contestability and fairness.

This is also relevant because **contestability and fairness both require users to make effective choices between the options available**, reflecting their relative value. And this will only occur if they make their decisions in the context of a suitable choice architecture. If they don't, and users instead stick with the gatekeepers' services even where these are less good, this will not facilitate the sort of dynamic and innovative environment that the DMA is seeking to achieve.

Thus, the design of suitable choice architecture is intrinsic to effective compliance with the DMA. But what does this mean in practice?

Overarching principles for effective compliance

For assessing the design of compliant choice architecture, we identify and discuss three legal principles and three economic principles.

The three legal principles we propose are: **effectiveness, proportionality, and non-discrimination** (that is, ensuring that choice architecture does not favour the gatekeeper).

A key issue highlighted in relation to proportionality is the potential tension between contestability and user autonomy.

For example, consider the browser choice screen that users must receive under Article 6(3). If the proprietary option is put top of the list of choices, then we would expect most users to choose it, implying little impact on contestability. On the other hand, if we prioritised contestability, the best approach might be to make the proprietary option fairly hard to find (for example, below the scroll), but this might make it hard to find for users that actively want this option, which could in turn harm user autonomy.

We conclude that it is useful to think about the proportionality principle as **requiring gatekeepers to comply with the DMA while respecting end user autonomy**.

The three economic principles proposed are:

- first, that gatekeepers should employ the 'attend, access, assess, act' (4 As) choice framework;
- second, that they should **carry out *ex ante* testing** to demonstrate the expected impact of their choice architecture; and
- third, that they should also evaluate this impact *ex post*.

The 4As choice framework is useful in thinking through the various steps in end users decision-making, and we discuss how it is important to consider the choice architecture relevant to each of these steps. For example:

- For those provisions that require the gatekeeper to mandate choice, it is important that end users give this choice sufficient *attention*. This will be more likely if the choice is prominent, well-timed, and impossible to skip.
- It is important that end users are able to *access* relevant settings in an intuitive and easy way, or perhaps multiple alternative ways.
- End users will need to be able to *assess* the available options effectively, which in turn means the information provided must be not only true, but also 'graspable'; there should be sufficient information but not too much; and there should not be any unfair framing that favours the gatekeeper's service, in terms of defaults, prominence, rankings, and so on.
- End users should be able to *act* on their choice easily, without having to make any further changes to their settings, without facing disproportionate warnings, and without facing nudges or prompts to change their minds. They may be encouraged to try an alternative option if they are informed that their choice is reversible.

None of this is straightforward. The impact of different choice architectures will be highly context-dependent. This is in turn why testing – both *ex ante* and *ex post* – will be so critical to effective compliance.

cerre Centre on Regulation in Europe

CHOICE ARCHITECTURE FOR END USERS IN THE DMA

AMELIA FLETCHER

2. CHOICE ARCHITECTURE IN THE DMA

2.1. What is Choice Architecture?

"Choice architecture" is a neutral term, which simply describes the way in which information and choices are presented to end users. This can include a wide variety of aspects relating to how choices are 'framed', including the number and ordering of options, whether any options are set as 'defaults' or made more prominent, the information provided at the time of choice, the information and screen provided prior to that choice (which can have 'priming' effects), the wording, the timing and frequency of choices, illustrations, and colours used, and so on.[41]

Why does this matter? Because it is well understood that **these elements can steer user decision-making, subtly but powerfully**.[42] Indeed, in some situations, this steering may be sufficiently strong that users are not even aware that they have a choice. Such effects are especially important in relation to the digital gatekeepers.

First, we know that **many end users are inexpert in the choices** they will need to make on digital platforms and that decision-making can be a mental burden, with people typically disinclined to spend significant time or energy in making choices. This can lead to end users being disinclined to act at all, sometimes called the "status quo effect".

It can also lead to end users utilising a variety of decisional short cuts, sometimes known as heuristics, which in turn mean that their choices may be influenced by the way in which options are framed. This can lead to a variety of other well evidenced effects such as the "default effect" (the tendency to accept the default), the "ranking effect" (the tendency to choose higher ranked options), the "salience effect" (the tendency to choose more salient or prominent options), and so on.

Second, we know that the digital gatekeepers are well-positioned to identify and implement choice architectures that most effectively steer end users in the way that the gatekeeper desires. They have full control over the choice environment that lies between end users, on the one hand, and business users and third-party services, on the other. They are also able to finetune that environment through extensive testing. This includes trialling different interface designs on live users, rather than in an artificial test environment, using analytical techniques such as A/B and multivariate testing.

This meticulous design of the choice architecture facing end users can have **positive effects**. For example, we know that online platforms put substantial effort into designing their systems in a user-friendly way. They seek to ensure that end users enjoy a smooth consumer[43] journey, without having to make too many active choices, and the product works well 'out of the box'. It is simply not realistic

[41] The DMA in fact refers to 'interface design' rather than choice architecture. We treat these terms as synonymous in this context.

[42] For the relevant evidence on a variety of behavioural effects relevant to competition, see CMA (2022), *Online Choice Architecture: How digital design can harm competition and end users*, Discussion Paper.

[43] Note that we use the terms 'consumer' and 'end user' interchangeably throughout this document as, for the purposes of the issues discussed, the two concepts are broadly the same. Where there is any divergence, however, the wording should be taken to refer to 'end users', since this is the term used in the Digital Markets Act.

to ask end users to make choices in relation to the many different design options that a gatekeeper's service might incorporate. Not only do end users not have the required expertise, but also there would simply be too many decisions. End users would likely end up exhibiting 'choice fatigue' (i.e. becoming mentally exhausted by having to make too many decisions) and perhaps start using rules of thumb or making mistakes, if they were forced to make a series of decisions about the detailed design of their user interface. They may even be deterred from using the product (or from switching product) entirely.

In general, many of the design decisions made by gatekeepers will be *fixed*, in the sense that end users cannot alter them even if they wish to do so. But some decisions, particularly in relation to software options, remain *flexible*, in that the gatekeeper will set a 'default' but end users retain the option to alter this. While there are benefits to retaining such flexibility, the associated choice architecture is critical to its overall effect. For example, choice architecture can have **negative effects** if it steers users towards a gatekeeper's own services when these are not necessarily the user's preferred options, or if it is difficult for users to alter the settings. When choice architecture has such negative effects, it is sometimes referred to as containing "**dark patterns**". And these can affect all users, not just more vulnerable users.[44]

Behavioural insights are relevant to the impact of such dark patterns. For example, we know that many end users – having been provided with a default option – will **simply adopt it (the "default effect") and will not revisit that decision (the "status quo effect")**. Users may also perceive the default option to be an implicit endorsement or recommendation by the gatekeeper. This effect will tend to be exacerbated if end users are unaware that they can change their default, if it is unclear how to do so, or if doing so involves a long and complex process.

Adopting and sticking with the gatekeeper's proprietary service can be detrimental to end users if they would be better off with an alternative option. Perhaps more critically (especially in the context of the DMA), it **can be harmful for competition**. If a gatekeeper makes its own proprietary service the default option, third-party rivals will struggle to gain end-user attention or gain market share.

Similar issues can arise if the gatekeeper favours its own products or services in other arenas where end users have a choice, such as in-app stores or online marketplaces. For example, we know that rankings can have a positive effect in helping end users choose from a wide range of options.[45] But equally, we know that end users are more inclined to choose higher ranked or more salient options (the "ranking effect" and "salience effect"). Thus, self-preferencing by a gatekeeper can take the form of ranking its own products or services more highly, making them more prominent as options, or otherwise 'priming' end users to select the gatekeeper's services.

[44] Zac, A. et al (2023), "Dark Patterns and Online Consumer Vulnerability", *Centre for Competition Law and Policy Working Paper,* CCLP(L)55.

[45] For a discussion of both positive and negative implications of recommender systems, see Fletcher A et al (2023), "Recommender Systems and Supplier Competition on Platforms", forthcoming in *The Journal of Competition Law and Economics*. Available on SSRN.

2.2. Relevant DMA provisions

Given the important positive benefits of some key elements of choice architecture, the DMA does not seek to change the situation entirely. **Default settings and rankings are not prohibited. Rather, the DMA seeks to limit the extent to which the gatekeeper has an intrinsic competitive advantage and to expand the role of consumer choice in some specific ways**.

In fact, the DMA includes provisions that address choice architecture design issues in relation to three core contexts.

1. **Enabling end user choice**: Provisions that simply require the gatekeeper to *enable* end user choice.
2. **Mandating end user choice**: Provisions that further require the gatekeeper to *mandate* end users to make a choice.
3. **Enabling third parties to offer choice:** Provisions that require the gatekeeper to *enable third parties* to offer end user choice or even mandate it.

The key provisions that relate to **enabling end user choice** are:[46]

- *Article 5(5):* End users should be allowed to access and use, through the gatekeeper's core platform services (CPS), any content, subscriptions, features, etc, that they have acquired directly from a third-party business user when using their app.
- *Article 6(3):* End users should be able to easily uninstall apps.
- *Article 6(3):* End users should be easily able to change default settings on gatekeeper's operating system (OS), virtual assistant, and web browser, where these otherwise steer end users to services provided by the gatekeeper.
- Article 6(4): End users should be able to install and effectively use third party apps and app stores, using a gatekeeper's OS, without using the relevant CPS (i.e. app store) of that gatekeeper.
- *Article 6(4):* End users should be able to set that downloaded app or app store as their default easily.
- *Article 6(6):* End users should not be restricted in their ability to switch between, and subscribe to, different apps that are accessed using the gatekeepers' CPS.

[46] **Article 6(7)** is not listed here, as it contains no explicit role for end user choice. However, the requirement for "effective interoperability" arguably requires that third party providers of services and hardware, interoperating with the gatekeeper's CPS, are placed on an equal footing to the gatekeeper's own services in terms of providing and communicating choices for end users. This provision will be discussed in detail in another paper in this series.

- *Article 6(9):* End users should be able to port their data, including to third parties where this has been authorised by the end user.
- *Article 6(13):* The conditions for an end user terminating a CPS may not be disproportionate and must be exercisable without undue difficulty.
- *Article 7(7):* End users must remain free to decide whether they make use of the new interoperability of interpersonal communications services, to be introduced under Article 7.

The key provisions that relate to **mandating end user choice** are:

- *Article 5(2):* Gatekeepers may not process, combine or cross-use end users' personal data or sign them into new services, unless the end user has been presented with a specific choice and provided consent.[47]
- *Article 6(3):* Gatekeepers must prompt end users, at first use of search engine, virtual assistant, and web browser, to choose a default option for this service from a selection of the main available providers.

The key provisions that relate to **enabling third parties to offer choice** are:

- *Article 5(4):* Gatekeepers must allow third parties, free of charge, to communicate and promote offers to end users, and to conclude contracts with those end users, regardless of whether they use the gatekeeper's CPS to do so.
- *Article 6(4):* The gatekeeper shall not prevent downloaded third-party apps and app stores from prompting end users to consider setting their app or app store as their default.

It should be noted that there are many more requirements relating to enabling choice than to mandating it. This reflects the fact that many end users will not want to be forced to make choices, while others will proactively wish to make them.

It should also be noted that enabling, and even mandating, end user choice is not the same as imposing specific choices on those end users. If an end user is given a fair and effective choice and still opts for the gatekeeper's services, this should not be viewed as noncompliant with the DMA. On the other hand, given that end users are likely to have diverse preferences, zero take-up of alternative options might at least raise questions as to the effectiveness of the choice architecture.

[47] This article is discussed within another paper in this series, so we do not list it here. (see de Streel, A. and G. Mont (2023) "Data-related obligations in the DMA: remedy design and link to other EU rules", CERRE draft issues paper). Choice architecture issues are relevant to such consents, as discussed in a recent joint paper by the UK Competition and Markets Authority (CMA), Information Commissioner's Office (ICO) and Digital Regulation Cooperation Forum (DRCF). See CMA/ICO/DRCF (2023) Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information.

3. THREE LEGAL PRINCIPLES FOR CHOICE ARCHITECTURE DESIGN UNDER THE DMA

It is important to read the above provisions in the context of the wider DMA regulatory framework, and in particular in relation to three core legal principles of effectiveness, proportionality, and non-discrimination.

3.1. Effectiveness

Central to the DMA is a focus on **effectiveness**. In particular:

- Article 8 (on compliance) requires that gatekeepers ensure that implementation is **effective in achieving the aims of the specific provisions and also the objectives of the DMA** – fairness and contestability.
- A number of specific Article 6 provisions also mention the need for effectiveness.[48]

As discussed above, suitable choice architecture will be critical to the effectiveness of the DMA in achieving fairness and contestability, since both require users make effective choices between the options available, reflecting their relative value. If users instead stick with the gatekeepers' services, even where these are less good, this will not facilitate the sort of dynamic and innovative environment that the DMA is seeking to achieve.

This expressly prohibits any circumvention behaviour that undermines effective compliance, and notably:

- Article 13(4) makes specific reference to the importance of behavioural techniques and interface design for effective compliance, while Article 13(6) prohibits gatekeepers from making choices unduly difficult, including "by offering choices in a non-neutral manner" or subverting end users' "autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface."[49]

3.2. Proportionality

Proportionality is also relevant to the implementation of the DMA. This is clear within the DMA itself (see Article 8 and Recital 29). Proportionality plays a role in the limited defences provided within the

[48] Articles 6(4), 6(7), 6(9), and 6(10). For further discussion on this, see Fletcher, A. (2022). "Behavioural insights in the DMA: A good start, but how will the story end?". *Competition Policy International*.

[49] Note that there is similar reference to interface design in the Digital Services Act (Article 25(1)): "Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."

DMA obligations.[50] There is also a general principle of proportionality in EU law.[51] The DMA should thus be interpreted as requiring gatekeepers to implement the provisions above in a way that is effective but not disproportionate in achieving the objectives of the DMA.

But what does this mean in practice? What it clearly does not mean is that gatekeepers are free not to comply with the DMA provisions if their costs of doing so exceed the expected benefits in terms of fairness or contestability. This would be inconsistent with the rule-like nature of the provisions and the lack of any explicit efficiency defence within the DMA. A better reading of the proportionality principle is that **the interpretation and implementation of the DMA's obligations should not exceed what is necessary to achieve its objectives**.

But what does this mean in the context of choice architecture design? We know that it is difficult, if not impossible, to design choice architecture that is fully effective in driving good decision-making, let alone contestability or fairness. As such, the most that can really be hoped for, in the context of choice architecture design, is not contestability and fairness but *more* contestability and fairness. But this might in turn suggest that the principle of proportionality has limited relevance to choice architecture design, since it is hard to think of measures that would *go beyond* what is necessary to comply. Nonetheless, there seems to be one key element of choice architecture design where the proportionality principle seems very relevant. This relates to how well the choice architecture delivers end user autonomy.

There can potentially be a **tension between promoting contestability and end user autonomy**. Consider, for example, the requirement under Article 6(3) whereby a designated browser must offer end users an upfront choice of search engines, and not just default them into using its proprietary search engine. But how is this to be designed, and in particular how should the gatekeeper's own service be ranked? In practice, there is likely to be a spectrum of possible options.

- At one end of the spectrum, it could theoretically be argued that, given the popularity of the gatekeeper's proprietary search engine, it should be ranked first on the list of options as this would best enable end users to choose their favoured option. However, this seems unlikely to be compliant with the DMA. The current popularity of specific search engines reflects over a decade of users being steered towards those services. Ranking these tops is unlikely to be effective in disrupting the status quo and enhancing contestability. Given the existence of strong 'ranking effects' – whereby users are more likely to choose a higher ranked option – end users would be highly likely to select the proprietary option.

[50] For example, Article 6(4) requires gatekeepers to allow the installation and effective use of third-party apps and app stores that can be accessed separately from the gatekeeper's core platform service. However, the gatekeeper may nonetheless take measures to protect the security and integrity of its own hardware and software, so long as they are 'strictly necessary and proportionate'. The same applies to interoperability obligation at Articles 6(7). Article 7(7) includes a similar proportionality measure in relation to interoperability of communications services, which refers not only to integrity and security but also privacy.

[51] Art. 5(4) TEU provides that ' Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties'.

- At the other end of the spectrum, given the very strong incumbent position of such a proprietary search engine, it could be argued that the impact on contestability would be maximised if it was made really quite difficult for end-users to find that proprietary search engine. This might, for example, be achieved by completely randomising the ordering across a wide range of options. This would arguably be good for contestability but less good for end user autonomy.

This raises the question of where on this spectrum the DMA expects gatekeepers to locate themselves in terms of the measures they take. **We consider that it is useful to think about the proportionality principle as requiring gatekeepers to comply with the DMA while respecting end user autonomy**. What does this mean in practice? Gatekeepers should certainly not seek to exploit behavioural insights to undermine user autonomy. However, they should also not be expected to limit end user autonomy unduly, in the name of contestability or fairness.[52]

In the example above, if the proprietary search engine was made too difficult to find, this could in fact be detrimental for those end users who would prefer this option. This would seem to act counter to the weight placed by the DMA on interface design not subverting or impairing user autonomy.[53] It is therefore arguably disproportionate to require gatekeepers to design their choice architecture in this way. How might proportionality be achieved in practice? Ideally, the chosen ranking approach would enable users who specifically want the gatekeeper's service to find it, but otherwise promote contestability to the largest extent possible. One natural option might be an alphabetical listing. However, while this would be easy to use and thus good for end user autonomy, it risks favouring those providers who happen to lie higher up the ranking alphabetically.

Empirical testing should be useful in identifying where the right balance is struck. For example, if those users who specifically want a proprietary search engine are found to be able to identify and choose this option even when it lies 'below the fold, then this would arguably strike the right balance.[54] If not, some form of stratified randomisation may be more appropriate (whereby the top, say, 5 options are listed first, but their order randomised, then the same for the next 5, and then the same for any 'long tail').

3.3. Non-discrimination in Choice Architecture

There is a real risk of gatekeepers self-preferencing in their design of choice architecture. This can take many different forms, from making its proprietary service a default, to ranking it highly, to making it the most prominent option, to making it easier to access (for example, requiring fewer clicks), to 'priming' users by preceding the choice with screens that focus on the gatekeeper, and so on.

[52] Note that end user autonomy does not appear to be covered by the DMA objective of 'fairness', since this seems to relate only to the relationship between gatekeepers and their business users. See Recital 33.

[53] Recital 60 and Article 13(6).

[54] A recent experiment commissioned by BEUC found that placing a gatekeeper' service 'below the fold' was useful in encouraging users to explore other options, while not deterring those who were keen to choose that service. BEUC (2023) Examining the Design of Choice Screens in the context of the Digital Markets Act.

While there is no general principle of non-discrimination (or neutrality) within the DMA, there are two key reasons for considering it as a core principle, at least in relation to choice architecture.

The first is the language within Article 6(5) and also the associated Recital (52):

- *Article 6(5):* Prohibition on self-preferencing in ranking (and related indexing and crawling); and requirement to apply transparent, fair, and non-discriminatory conditions to such ranking.
- *Recital 52: "Ranking should in this context cover all forms of relative prominence, including display, rating, linking or voice results and should also include instances where a core platform service presents or communicates only one result to the end user. To ensure that this obligation is effective and cannot be circumvented, it should also apply to any measure that has an equivalent effect to the differentiated or preferential treatment in ranking."*

The second is the wording in *Article 13(6)* – mentioned above – which prohibits gatekeepers from making choices "*unduly difficult, including by offering choices in a non-neutral manner*" or subverting end users' "*autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface*."

Together, these elements cover the most possible types of choice architecture relevant to the DMA and suggest that **non-discrimination** should be viewed as a **core principle in relation to choice architecture**.

In practice, **non-discrimination can be a complex concept to apply**. Any choice architecture will, by its nature, have more prominent and less prominent options and thus have an effect in steering end users' choices. This is especially likely to be true where there are many available options. As such, and noting the contestability and fairness objectives of the DMA, we propose that this concept should in practice be construed as meaning '**avoiding discrimination that favours the gatekeeper'** and this is the interpretation we assume below. [55]

To achieve this, **two elements are involved**:

- *The design element***:** Designing the choice architecture itself so that it is **steering users as little as possible** (noting that it is impossible to entirely prevent all such steering); and
- *The allocation element:* Ensuring that **access to the more popular positions** within the choice architecture is **allocated in a non-discriminatory manner**.

These two elements are complementary and both are important.

In relation to the allocation element, we note that there are also a variety of complex issues arising. For example, Article 6(5) clearly prohibits gatekeepers from using criteria that directly favour their

[55] Note that discrimination in the context of online platforms is sometimes also referred to as "intermediation bias". This was discussed in a 2019 CERRE paper on which this current paper builds. (Feasey, R. and J. Krämer (2019) "Implementing Effective Remedies for Anti-Competitive Intermediation Bias on Vertically Integrated Platforms", *CERRE Report*.

own products and services. But what about criteria that indirectly favour them? For example, suppose that an online marketplace bases its rankings partly on speed of delivery, a factor that it believes its customers value highly, but that this in turn advantages products utilising that marketplace's highly effective proprietary logistics service. Does this count as non-discriminatory? How could this be demonstrated empirically? As discussed elsewhere, paid-for rankings raise especially complex issues in this context.[56]

Given these issues arising in relation to the **allocation element**, we consider that there is likely also to be a benefit in seeking to increase non-discrimination within the **design element** of the choice architecture. This design element is the core focus of this paper.

[56] See fn. 55. Also, Fletcher, A. et al (2023). "The Effective Use of Economics in the EU Digital Markets Act". *Jour. of Competition Law & Economics*, forthcoming.

4. THREE ECONOMIC PRINCIPLES FOR CHOICE ARCHITECTURE DESIGN UNDER THE DMA

A key challenge for the various DMA provisions outlined above is that their effectiveness in delivering the objectives of the DMA depends critically on the extent of their impact on end user behaviour. For example, enabling end users to switch their defaults will only be effective in enhancing contestability if end users take advantage of these options.

But as has already been highlighted, there are a variety of behavioural factors that can restrict consumers from making effective choices, or indeed from making choices at all. Fletcher and Vasas (2023)[57] discuss several relevant behavioural insights in some detail. These include ranking effects, saliency effects, default effects, status quo effects, framing effects, social cues, obfuscation and shrouding, information overload, choice fatigue, complexification, and timing effects. These can, for example, lead to users failing to choose the option most ideal for them, and instead sticking with the default or status quo option; choosing the highest ranked, most salient, or least complex option; or simply making mistakes. These effects can all be exacerbated when users have limited time, cognitive bandwidth, capability, context, or motivation. A key conclusion of that paper is that the **design of choice architecture can therefore be critical to the extent – and quality – of consumer choice activity, and thus to the effectiveness of the DMA** in achieving its objectives.

But what does this mean more generally in terms of key principles for choice architecture design? In this section, we propose three key principles for choice architecture design under the DMA. Specifically, that gatekeepers should employ the 'attend, access, assess, act' choice framework, carry out *ex ante* testing, and evaluate impact *ex post*.

4.1. Employ the 'Attend, Access, Assess, Act' Choice Framework

When examining potential barriers to effective end user choice, we consider that it will be important to employ the '*Attend, Access, Assess, Act*' framework of consumer choice, also known as the '4 As' framework.[58] This will be key to ensuring that the choice architecture adopted is appropriately targeted at effectiveness, proportionality, and non-discrimination.

This framework highlights that end users go through four key steps when making choices:

1. They clearly need to **attend** to (or engage with) the market in the first place.
2. They then need to **access** information about the products (goods or services) available in the market.

[57] Fletcher, A. and Z. Vasas (2023). "Implementing the DMA: The role of behavioural insights." Forthcoming in *The Oxford Review of Economic Policy*. Forthcoming in *The Oxford Review of Economic Policy.* Working Paper available on SSRN.

[58] See Fletcher, A. (2021). "Disclosure as a tool for enhancing consumer engagement and competition." *Behavioural Public Policy, 5*(2), 252-278. Note that an early version of this framework was developed by the UK Office of Fair Trading (now the Competition and Markets Authority).

3. They then need to **assess** that information, in terms of making comparisons across the various products and determining which best suits their preferences.

4. Finally, they need to **act** on that information, by purchasing or switching to their preferred product, and thereafter using it.

This framework is useful in focusing attention on ensuring that each step is working well. In the following, we utilise it to draw some lessons for each of the categories of provision described in Section 2.2.

Note that the first step (attend) is not necessarily relevant to those DMA provisions that relate to enabling end user choice, as these provisions apply to end users who are already actively seeking to make a choice. However, the other three steps clearly apply, and all steps apply to the provisions relating to mandating end user choice.

4.1.1. Enabling end user choice

As highlighted above, several DMA provisions are designed to make it easier for end users to make choices, whether this be to utilise third party services, to change default settings, to download third party apps and app stores, to port data, or to switch or terminate services. The **access, assess** and **act** steps are all relevant here.

Access

First, end users must be able to **access** relevant information about options. In the context of the DMA provisions, this means that, for any choice, it should be:

- clear that a choice can be made;
- clear that a choice can be reversed;
- easy to find **where** the choice can be made; and
- clear **what the options are**. Note that these choices may be binary (e.g. switch/don't switch) or multiple (e.g. choice of search engine)

For example, in the context of some of the relevant articles listed above, this could mean:

- *Article 6(3):* The option to uninstall apps should be easy to access (for example by pressing on an app's icon) and the consumer journey should be the same for third party apps as for proprietary apps.
- *Article 6(3)/6(4):* It should be straightforward for users to find where to change the default settings on gatekeeper's operating system, virtual assistant, and web browser. There should be no distinction on the basis of how the app (or app store) was downloaded. Note that making access straightforward may involve allowing multiple routes of access. For example, if a user wishes to alter the default web browser used by their voice assistant, this should

arguably be possible to achieve via the settings for the web browser and also via the settings for the voice assistant.

- *Article 6(4):* Any third-party apps and app stores that have been downloaded not through the gatekeeper's own services should be located alongside (and usable in the same way as) those that have.
- *Article 6(6):* It should be straightforward for end users to switch between, and subscribe to, apps that are accessed using the gatekeepers' CPS. Proprietary apps and third party apps should be treated in the same way.
- *Article 6(9):* It should be clear to end users how to port their data in relation to any particular service. If consumers are asked to confirm that they understand that a third party will be porting their data, this should be straightforward. It should also be straightforward to terminate the porting arrangement at any point.
- *Article 6(13):* It should be straightforward for an end user to find where to terminate a CPS.

Assess

Second, consumers should be able to **assess** the available choices, on a reasoned and undistorted basis. This is as true for both binary choices as it is for choices with multiple options. Note that this will naturally require the provision of information, in relation to both the context of the choice being provided and the options available. It also requires that the choice architecture allows for non-discriminatory choice. This in turn means that:

- Information provided should be both **true and 'graspable'** by an average end user. It should avoid language that is too long, complex, or legalistic to be easily understood when going through the user journey.
- There should be **sufficient information** about the options to help in making a reasoned choice. Where relevant, this should include information about the consequences of the choice, including its reversibility. For example, what happens if an end user uninstalls an app? There should not, however, be too much information as this could create information overload, but consideration should be given to including shortcuts (to further information if required).
- Consideration should be given to whether decision-making is likely to be most effective when choices are **binary** ('make this service my default' vs 'retain my current default') or when they include **multiple options** ('which of these services would you like to make the default?').
- The options should not be ranked, made prominent, made the 'default', or otherwise **framed** in a way that unfairly favours the proprietary or default or status quo offering (or indeed any other offering).
- The extent of choice should reflect the **full range of options available** (whether pre-installed or downloaded) without consumers having to carry out any additional actions.

- All language should strike a **neutral tone**. It should avoid instilling undue concern, uncertainty or doubt. Any **warnings should be accurate and not disproportionately prominent**.

Act

Finally, consumers should be able to **act** on their assessment. That is, they should not be deterred from choosing their preferred option, or from sticking with it. For example,

- There should be **simple and easy navigation**, with no unnecessary steps, delays or friction in the user journey.
- The complexity of making choices (numbers of clicks, warnings, and so on) should **not differ between proprietary and third-party** options.
- Where a default setting could impact multiple access points (for example, a search engine default), the end user should be able to change the default **across all access points at once**.
- It should be clear that any choice is **reversible**, and any such reversion should be easy. (This will tend to encourage action, as opposed to cautious inaction).
- Any action (e.g. to change default) should **not be undermined by** the gatekeeper then **prompting** the end user to change back (or switching the end user back without asking).
- Products and services chosen should then **work automatically**, without end users having to make further changes to settings.
- There should be **no nudges or prompts** about the greater interoperability, or superior performance, of the gatekeepers' own services.

These various requirements are widely applicable to the various provisions listed above.

4.1.2. Mandating end user choice

The above all apply in situations of 'mandated user choice', but so does an additional aspect of decision-making, the need to ensure that end users **attend** to the need to make a choice.

This is especially relevant in the context of the **active choice of default settings** required under Article 6(3). This provision is designed to deal with the natural tendency of end users to accept the default option (default effect) and then stick with it (status quo effect), even when there are alternative options that would suit them better.

However, just providing a prompt to make a choice may not actually be enough to drive active choice, especially if users are focused on doing something else. For example, if an end user opens up a particular browser to do a search and is then prompted to choose a search engine or browser, they

may well opt to do this as quickly as possible – to get on with the search – rather than seriously considering the choice.[59]

In this context, the key issues are likely to be:

- **Prominence and clarity of the active choice**: Is it possible for users to click through it so fast that they barely notice it, or to skip it entirely?
- **Extent of choice**. It is important that the number of options should not be unduly limited as this not only limits access by third parties but also risks creating 'scarcity effects' whereby users infer value from the mere scarcity of an option.[60]
- **Extent of information***:* As above, it is important that the information provided is true and 'graspable', genuinely aiding decision-making while avoiding information overload. This is especially important in the context of mandated choice screens, given that end users will not have proactively sought out the choice. It is important that they understand the choice they are being asked to make, as well as the options. It may be important that the options include short descriptions and logos.[61] Social cues, such as user rankings, may be valuable, but take care to ensure that these do not unduly favour incumbents.
- **Non-discrimination across options**: If one option is particularly prominent or ranked highly, users are especially likely to choose it, especially if they are in a rush and not focussed. This can also relate to information provided before the choice screen that has the effect of 'priming' the user to accept a particular option.
- **Timing of the choice**: Is it provided at a point where users are likely to consider it relevant and likely to spend time thinking about the options?
    - It is useful that, on the date the DMA comes into force, this should act as a trigger for all relevant device users to receive the required choice prompt. This will provide a useful window within which third parties can market their services more widely, thereby helping users to make a considered choice.[62]

[59] For example, the Mozilla research cited above found evidence that interrupting the user flow in this way substantially increased the extent to which users retained the pre-installed default. See fn. 60.

[60] At the other extreme, if there are too many options, there could be a risk of choice overload. This can potentially be overcome through the use of 'ordered groups' (eg the 5 most popular options first, followed by the remaining options). However, recent experimental research commissioned by Mozilla found no evidence of such choice overload. See Mozilla (2023), Can Browser Choice Screens Be Effective? Experimental Analysis of the Impact of their Design, Content and Placement.

[61] The BEUC research referred to at footnote 54 also found that end users were more inclined to choose the gatekeeper's service in the absence of logos. Their interpretation of this finding was that "*When users are unable to locate their preferred option immediately, they may feel disorientated and become even more resolute in finding a familiar choice*".

[62] In this context, it is important that prior views of existing choice boxes are not accepted as relevant for DMA compliance.

- After that, on an ongoing basis, the best time to present options may well be at the point of setting up a new device, since users are more likely to be in the right mindset at that point.

- **Information provided to the user immediately prior to making the choice:** Is the choice provided at a time when the end user has seen the name and logo of the gatekeeper on the several screens preceding the choice? If so, this may have an unhelpful 'priming' effect on their choice.

- **Frequency of the active choice:** If consumers are asked to make the same choice too often, they may exhibit choice fatigue. However, given the importance of ensuring that the DMA is effective in driving contestability, there would be merit in their being asked on a reasonably frequent basis (so long as they retain the gatekeeper's proprietary service). At a minimum, it is important that users are asked *every time* they set up a device. That is, even if users choose to use their previous settings, they should still be required to re-consider their choice of default browser, search engine, and virtual assistant (as relevant).

- **Ability to ask to be prompted again:** if the timing is not good, end users may prefer to delay the choice rather than make it too quickly. In this case, an option to 'ask me again tomorrow' (or such) may be valuable. However, it is important that this option is not over-used. For example, users should not be encouraged to procrastinate indefinitely. Moreover, providing such an option at the set-up stage could result in users delaying the decision to a time when they are even less likely to make a considered choice. This would not be helpful for compliance.

4.1.3. Enabling third parties to offer choice

For those provisions which are designed to enable third party service providers to offer choice to users (Articles 5(4) and 6(4)), much of the above will apply. But in addition, two other issues arise:

- The ability of third parties to control the content and format of the choice.

- The frequency of prompts/communications.

The content and format of the choice are clearly relevant to ensuring that end users are able to *access* and *assess* the options, and are not steered towards choosing (*acting*) any particular option in an unduly discriminatory way. The frequency of prompts is relevant to ensuring that end users *attend* to the available choice at all.

Given the DMA's objectives of fairness and contestability, one might think it would be **appropriate for third parties to control the content and format of these choices, and also their frequency**, since they will have a strong incentive to encourage end users to consider their service as a default. However, this is a situation where the discussion above relating to end user autonomy may be relevant. In terms of format, there may be benefits to end user comprehension if they always receive such prompts in broadly the same format. Moreover, there is some risk that third parties design their prompts to induce end users to make choices that are not in their own interest.

Likewise, in terms of frequency, if users are subjected to overly frequent prompts, they may suffer the effects of badgering or notification fatigue, becoming less attentive and more likely to make mistakes. In our previous paper, we highlighted the risk of third party "slamming" whereby end users are effectively switched without even noticing (as has sometimes occurred in telecoms markets). It is unlikely that responsible services would behave in this way, as it would likely harm their reputation, but less responsible services could be less restrained.

There is a **difficult balance** to be struck here. To the extent that any harmful conduct by third parties breaches other regulations (such as consumer law), the gatekeeper should have the power (and indeed a duty) to address such conduct. However, to the extent that such conduct is legal (but harmful), it may make most sense for third parties to retain overall control but within certain parameters set by the gatekeeper (and these would in turn need to be objective and proportionate). Equally, if the gatekeepers do retain control over the format, it is important that there is some potential for third party customisation.

Finally, in order to ensure that prompts are well-framed to generate effective end user decision-making, it is important that third parties able to target them specifically at users that have not already set their service as a default. It is also important that the prompt takes users directly to the relevant choice screen, as opposed to the general settings menu which they may find hard to navigate.

4.2. Carry out Ante Testing to Assess Likely Impact

Given that compliance with the DMA requires ensuring effectiveness of measures in delivering contestability and fairness, it is important that this is assessed empirically.

As should be clear from the discussion so far, the effectiveness of different choice architecture designs will depend critically on how well they enable effective end user decision-making. And while there is substantial general evidence underpinning certain behavioural insights ('status quo effects', 'default effects', 'prominence effects'), it can be hard to know how significant a role such effects are liable to play in any particular choice context. Moreover, many of the design issues highlighted have a 'goldilocks' aspect, in that end users need just enough (e.g. information to allow reasoned choice) but not too much (e.g. to avoid information overload). At the same time, as we have also discussed, it is also important that choice architecture respects the autonomy of end users, even if their choices happen to be bad for themselves and/or contestability. This further complicates the design of effective choice architecture. This means that **experimental *ex ante* testing will be critical, if choice architecture is to be designed that is genuinely effective, proportionate, and non-discriminatory**.

Such *ex ante* testing can take three key forms:

- **Lab experiments:** These are not necessarily done in the laboratory – they are often done online – but they involve participants being asked to make choices in a more clearly experimental context. The participants know they are part of an experiment and that the choices aren't real (albeit they may be given real incentives, most usually in the form of cash). The attention they give to their decision-making may therefore be rather different from that of real end users in a real context, which can affect the extent of behavioural effects observed.

- **Field trials:** These are also known as 'randomised controlled trials' (RCTs) or 'A/B' or 'multivariate testing'. They involve trialling different options with real end users, in real choice environments, who are unaware they are part of an experiment, and analysing their reactions.
- **End user surveys:** Surveys can provide useful directional indicators of how end users may be expected to react to particular measures, and can also be valuable for collecting qualitative information. However, it should be noted that there can often be a substantial difference between end users' stated intentions and preferences and their actual behaviour. Surveys can be especially valuable in following up lab experiments or field trials, for example by asking participants whether they are content with the option they chose or the information they were provided with. Note that field trials and lab experiments can usefully be supplemented with survey questions, for example, to elicit how the end user feels about the choice they have made, the options they were given, and how these were framed. Such survey responses can be especially valuable for assessing whether there has been any restriction of end user autonomy (as discussed above).

Of these three approaches, field trials tend to deliver the most realistic results[63], but they can typically only realistically be done by the gatekeepers, who thus control the experimental framework. Field trials may also be of limited value in assessing the effectiveness of different choice architecture options unless they are coupled with surveys. Third parties are most likely to need to rely on consumer surveys or lab experiments. These are less realistic but can generate cleaner results and important insights. Indeed, given that participants in laboratory experiments are typically relatively focused on the process, any mistakes they make may well be amplified in more realistic situations.

Under the DMA, gatekeepers are required to provide annual compliance reports. Since assessing compliance will necessarily involve assessing the effectiveness of choice architecture in achieving the objectives of the DMA, these reports **should be transparent about what the gatekeepers have done to test this and their rationale for the choice architecture then adopted**.[64]

Of course, testing takes time, and thus it may be unrealistic to expect the gatekeepers to have fully tested all aspects of their choice architecture prior to the implementation of the DMA. However, such testing can be continued over time.

The gatekeepers are the only parties that can carry out live field trials, and thus **they must have primary responsibility for this testing**. However, given the importance of ensuring that the testing probes the right questions, the **Commission will wish to oversee the testing programme – or nominate independent third parties** to do so – and may wish to approve and suggest changes to it.

[63] For a deeper discussion of the pros and cons of these three techniques, see Vasas, Z. (2023) "Do nudges increase consumer search and switching? Evidence from financial markets," *Behavioural Public Policy*, 7(3), 808-824.

[64] A number of past CERRE Reports have made similar proposals for the increased *ex ante* testing of interventions. For example Feasey, R. and J. Krämer (2020) "Implementing effective remedies for anti-competitive intermediation bias on vertically integrated platforms", *CERRE*; and Kramer, J,. (ed) (2020), "Digital markets and online platforms New perspectives on regulation and competition law", *CERRE* (see preface).

Input from interested third parties through market testing will also be critical, and it would be valuable for the Commission to consider how this can be best achieved.[65]

In this context it is noteworthy (and positive) that the DMA compliance report template[66] requires gatekeepers to report, for each measure: "*any type of market analysis or testing, in particular A/B testing or consumer surveys, that have been carried out to estimate the expected impact of the measure on the [DMA's] objectives*". The template also emphasises that the Commission may require specific testing in order to verify compliance. This could involve any or all of the three techniques described above.

In addition, the Commission and **third parties** may also wish to carry out their own *ex ante* testing, both to understand the likely impact of measures taken by the gatekeepers and more specifically to inform the Commission's oversight of the gatekeepers' own testing programmes.

4.3. Evaluate impact ex post

However, *ex ante* testing may not be possible in all cases. Even where it is, it may not provide an accurate view of likely impact. As such, to ensure that the DMA measures are effective, proportionate, and non-discriminatory, it will also be important for the gatekeepers (and third parties too where possible) to evaluate their impact *ex post*. This should enable learning about what works and what doesn't and thereby enhance the impact of the DMA in achieving its objectives going forward.

This need for ex post assessment is again reflected in the DMA's compliance report template, which also asks to see any analysis carried out in relation to actual impact.

A number of possible output indicators related to gatekeeper compliance in relation to choice architecture are discussed in CERRE's separate work on 'DMA Output Indicators."[67] This discussion is not revisited here. However, while those indicators will allow for the development of a basic and consistent picture of impact across gatekeepers, they will not be enough to fully assess the impact of different choice architecture designs. In order to ensure that they are complying effectively with the DMA, **the gatekeepers should also thus consider collecting and analysing additional *ex post* evidence.**

This may include:

- ***Ex post* evidence on the impact of different choice architecture designs:** For example, were all end users shown the same warnings in relation to downloading third party apps and app stores? If not, how many end users were shown each warning? And how many of these carried on regardless and completed the process?

[65] The UK CMA's experience in relation to market testing Google's Privacy Sandbox initiative may provide useful inspiration here.

[66] Commisstion Template for Compliance Report, Art.2.1.2. (ii) (o), see https://digital-markets-act.ec.europa.eu/template-compliance-report-under-digital-markets-act-published-2023-10-09_en.

[67] Feasey, R. and A. de Streel (2023). "DMA Output Indicators", CERRE draft issues paper. https://cerre.eu/wp-content/uploads/2023/07/CERRE-Draft-Issue-Paper-DMA-Output-Indicators.pdf

- **Consumers survey evidence**: For example, for a set of end users who received a choice screen, what proportion found it (i) comprehensible, (ii) useful, and (iii) engaging? What choices did they make? How hard did they think about it? Was this a new choice or the option they already used on a previous device? Are they happy with their choice? Do they intend to reconsider their choice within the next few months? Did they even notice they had a choice?
- **Retention evidence:** For example, of those end users who set an alternative to the gatekeeper's service as their default, how many of them had changed their default back within a year?

For all of the above, and where possible, it would also be valuable to collect figures from before any changes in choice architecture take place, to better enable the assessment of the impact of those changes.

cerre Centre on Regulation in Europe

HORIZONTAL AND VERTICAL INTEROPERABILITY IN THE DMA

MARC BOURREAU
JAN KRAEMER

1. GENERAL INTRODUCTION

This issue paper discusses some key issues and trade-offs that may arise in implementing the horizontal and vertical interoperability provisions of the DMA.

It builds on two previous CERRE papers, the 2022 CERRE report "Interoperability in Digital Markets", which discusses the pros and cons of mandating horizontal and vertical interoperability from an economic perspective, and the 2023 CERRE paper "DMA Horizontal and Vertical Interoperability Obligations", which addresses several issues of scope and implementation related to interoperability.

In this paper, we first discuss the implementation of the horizontal interoperability provision in the DMA (Article 7). We argue that horizontal interoperability will require proper management of user consent and careful interface design. We also argue that achieving horizontal interoperability poses significant technical challenges to: (i) resolve identities across providers; (ii) establish secure connections; and (iii) deal with malicious users. Solving these technical challenges will raise trade-offs for which there are no easy choices.

Second, we briefly discuss general principles for the implementation of vertical interoperability provisions, i.e., specifically Articles 6(4) and 6(7). Here, we argue for five principles, (i) screening of access requests, (ii) screening of access seekers, (iii) gatekeeper-led definition of interfaces, (iv) equivalence of input, and (v) a non-discriminatory choice architecture. We also emphasise that there can be interactions between the five principles so that they must be evaluated in concert, and not in isolation.

2. HORIZONTAL INTEROPERABILITY IN THE DMA

Article 7 of the DMA introduces a horizontal interoperability obligation for gatekeepers providing **number-independent interpersonal communications services** (NI-ICS).

This access obligation covers only a subset of **"basic functionalities**" of the messaging services offered by the gatekeepers. Within six months after the designation decision, interoperability should be available for text messaging and the sharing of images, videos and other files between individual users. In a second step, within two years of the designation decision, group chat should also be interoperable, and within four years, voice and video calls. Access must be provided **upon the request** of an access seeker and be **free of charge**.

The main objective of horizontal interoperability is to **improve the contestability of digital markets**. In the absence of interoperability, incumbent players (the gatekeepers) offering messaging services benefit from strong network effects that limit the contestability of the market. Interoperability is expected to level the playing field between incumbents and new entrants, as network effects are then shared among competitors and constitute a public good. We therefore expect **strengthened competition and reduced barriers to entry** in the market for messaging services. The successful entry of new players via (interoperable) messaging services may also allow them to expand gradually and develop their own ecosystem of complementary products. Therefore, opening up the messaging market to competition could also have a wider impact on digital markets.

At the same time, **horizontal interoperability may reduce multihoming** in messaging apps, which is another important driver of competition in digital markets. Moreover, as interoperability is also possible between gatekeepers, it could even **strengthen their position** vis-à-vis new entrants by making them more central for users. Overall, therefore, the impact of the horizontal interoperability provision on the contestability of digital markets remains uncertain.

3. HORIZONTAL INTEROPERABILITY: CONSENT MANAGEMENT AND DESIGN OF INTERFACES

3.1. Consent for Discoverability and Interoperable Communication

3.1.1. One-to-one communications

To implement interoperability between messaging services, user consent may be required at two different steps: for user discovery and for interoperable communication. We discuss both aspects in turn.

An important first step for the implementation of horizontal interoperability is to define how **user discovery** works, that is, to specify "the process of learning which service(s) a user uses and/or prefers" (Blessing & Anderson 2023).

Consider the following example. Alice wants to communicate with Bob, but they use different messaging services. Alice uses the service of a third party, *A*, while Bob uses the service of Gatekeeper, *B*. The only way Alice can reach Bob on *B*'s network is through interoperability. Gatekeeper *B* has published a reference offer (Article 7(4)), *A* has requested interoperability from *B* (Article 7(5)), and interoperability between *A* and *B* is operational. However, Alice must now "discover" that Bob is using *B*'s service in order to communicate with him via interoperability.

Bob could inform Alice of his identity on *B* during a **face-to-face meeting**, for example by using a QR code. By revealing his identity on B to Alice, Bob implicitly consents to being discovered by Alice and to communicating with her. This seems like the simplest solution from a consent perspective. One could also argue that it is sufficient to implement discoverability in this way, since the DMA does not require a specific solution for discoverability (it does not even mention it).

However, if users have to share contact information, there is a risk that interoperability will be little used. So, for interoperability to be effective, as required by the DMA, one could argue that user **discovery needs to be automated**, meaning that Alice's application (*A*) should be able to discover that Bob is using *B*. We now focus on this case where user discovery is automated.

A key question is whether Bob should **give his consent to be discoverable** on *B*, that is, opt-in to being discoverable by third-party applications like *A*.[68] Or should Bob instead be discoverable by default, while still having the ability to opt-out? BEREC, for example, considers this an open question (BEREC 2023, p. 25): "With regard to the data sharing and authentication among different interoperable services, the consent of the users to approve the exchange and processing of data to a third-party service needs to be clarified, e.g., if opt-out is possible or opt-in is obligatory." Moreover, Article 7(7) only requires that users "shall remain free to decide whether to make use of the interoperable basic functionalities," without specifying whether this should be done through an opt-in or opt-out regime.

[68] In this section, we focus on the issue of consent for discoverability. In Section 3.1, we also discuss the technical challenges of resolving identities across providers.

Requiring users to opt in to discovery imposes a cost on users, who may then prefer to remain undiscoverable (the default). So, there would be a risk that interoperability would be ineffective. In fact, email addresses are openly discoverable, which helps interoperability work seamlessly. Similarly, one of the reasons for WhatsApp's success is that user discovery is achieved automatically by searching users' address books and checking for contacts who use the application (WIK 2022).[69] For these reasons, some argue for an opt-out regime for interoperability. For example, users could be notified that they are discoverable and given clear instructions on how to opt out.

However, **we believe that users should be opted out of user discovery by default, and thus should give their consent explicitly for discoverability**.

The main reason for an opt-out regime is **user privacy**. Since the implementation of interoperability may imply the exchange of personal (meta) data between providers (see Sections 3 and 4 for a detailed discussion), the explicit consent of users may be required for privacy reasons alone. This is mentioned in the DMA, with Article 7(8) stating that the collection and exchange of data for the purposes of interoperability must comply with the GDPR and the ePrivacy Directive. Similarly, Recital 64 states that "interoperability should be without prejudice to the information and choices to be made available to end users of the number-independent interpersonal communication services of the gatekeeper and the requesting provider under this Regulation and other Union law, in particular Regulation 2016/679 [the GDPR Regulation]."

It is also a matter of **transparency** for users. With an opt-out regime, some users may simply not be aware that they are "discoverable" by users of third-party messaging apps. The opt-in regime ensures that users are fully aware that they can be discovered.

Having established that users should give their consent for discoverability, the next question is **how consent should be given**.

One possibility is to **ask users to give consent for each gatekeeper messaging service that they use**. For example, Bob should give his consent to be discoverable on service *B*. If Bob uses service *C* from another gatekeeper, he should be able to give his consent to be discoverable on *C* separately. Indeed, some users may want to use different messaging apps for different purposes (e.g., one app for work and another for communicating with friends and family), and in some cases may only want to be discoverable "on-net" in a particular app (Blessing & Anderson 2023). Note that in the context of Article 7 DMA, user discovery only concerns gatekeeper messaging services, and thus in principle a few services, so such a solution seems feasible.

Consent could also be more fine-grained. For example, Bob might be perfectly fine with being discovered on *B* and *C* by users of the third-party application *A*, but he might be extremely reluctant

[69] Note that it is possible to send a message to someone who is not a contact (see, e.g., https://www.forbes.com/sites/prakharkhanna/2022/12/22/how-to-send-message-on-whatsapp-without-saving-a-number/?sh=59dca12d5c87https://www.forbes.com/sites/prakharkhanna/2022/12/22/how-to-send-message-on-whatsapp-without-saving-a-number/?sh=59dca12d5c87), though WhatsApp gives users some control over who can contact or call them. So, having a phone number as an ID facilitates discovery, but phone numbers only appear as contacts if they are provided by the user (e.g., by uploading a phone book).

to be discovered by users of another third-party application *D*. In other words, consent could be given for **each pair of messaging services**, involving a gatekeeper's service and a third-party service. However, this approach may be too complex for users.

This also raises the question of which providers are entitled to discoverability. For security or privacy reasons, it would make sense to **restrict discoverability to "legitimate" third parties**. One approach would be to have the gatekeepers define in their reference offers the security and privacy standards that the providers should meet in order to have their interoperability request accepted (under the scrutiny of the European Commission). Alternatively, an industry body could also play this role -- because of the negative externalities that malicious providers could create, the industry as a whole would have an incentive to coordinate and define such standards. On these questions, see also our discussion in Section 4.2.

Alternatively, instead of filtering discoverability by platform, users could opt in to discoverability by user or user type. For example, Bob could agree to be discoverable by all of his contacts, regardless of which service they use. However, this solution is unlikely to be practical, unless the same identifier is used across services (see Section 3).

A practical solution should give the user some flexibility without being too complex. A possible solution in this regard would be to notify Bob, when he opens his gatekeeper messenger service B, that B is now interoperable with the third-party service A, and to ask him if he wants to take advantage of this interoperability feature. In this way, Bob would "opt in" to interoperability, while being forced to make an informed decision.

In all cases, users must have the ability to revoke discoverability. For example, if Bob no longer wants to be discoverable (e.g., because he feels he has received too much spam from third parties), he should be able to do so. Concretely, this would mean that Bob is no longer discoverable on his app *B*, but also that third parties who previously discovered Bob should now "forget" that he uses *B*.

Now, consider that Bob has consented to be discovered on his gatekeeper app *B*. Alice can now communicate with him via interoperability from her third-party app *A*. In this case, should Bob also **consent to an interoperable communication** with Alice? Today, messaging services handle this question differently. For example, Wire and Element require consent to communication, while many other services do not.

One could argue that it is like on a telephone network: if Bob does not want to talk to Alice, he just does not reply. However, there is a difference: Alice's message can show up even if Bob does not want to talk and it could be spam or an abusive message. Of course, Bob could "block" Alice, but this would only be possible after the message has appeared, with all its possible annoyances or risks.

The importance of this second level of consent probably depends on how specific the consent for discoverability is. Let's say Bob has to agree to be discoverable by all users of all third-party platforms. Then, there is probably a role for consent to interoperable communications for Bob to filter incoming communications. Conversely, if Bob has consented to be discoverable specifically by Alice, then there is less need for consent to interoperable communication with her.

3.1.2. Group chats

So far, we have discussed the impact of discoverability on one-to-one communications. However, within two years of the designation decision, interoperability should also apply to group chats. We argue here that group chats present additional challenges.

Consider the following example (from Wiewiorra et al., 2022). As shown in Figure 1 below, there are two gatekeepers, *A* and *B*, that are subject to interoperability requirements, and a third party, *C*. We assume that *C* is interoperable with *A* and *B*, but *A* and *B* are not interoperable (because they have chosen not to request interoperability from each other).

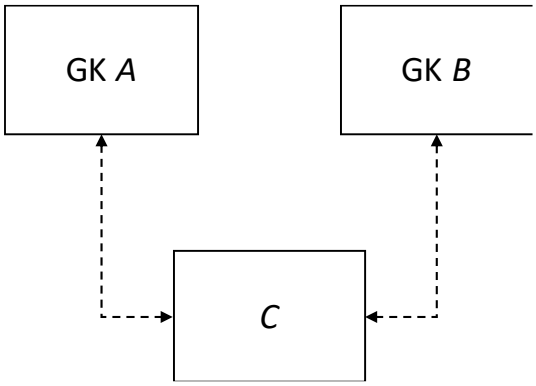


Figure 1: Example 1: third party C is interoperable with gatekeepers A and B, but A and B are not interoperable (example from Wiewiorra et al., 2022).

There is a group of users of *C* who want to chat with a user of *A*. Since C is interoperable with *A*, this group chat can work. However, what happens if they want to invite a user of *B* to join the group chat? *A* users and *B* users may have separately given their consent to be discoverable by *C* users and to communicate with them. However, *A* users have not given their consent to be discoverable by and communicate with *B* users, and vice versa.

Consider now this other scenario, with two gatekeepers (*A* and *B*) and three third parties (*C*, *D* and *E*). *C* is interoperable only with *A*, while *D* is interoperable with both *A* and *B*. Finally, *E* is not interoperable with any gatekeeper. Although there are five providers, four of which are interoperable with some others, in this scenario, group chats cannot occur with more than two providers.

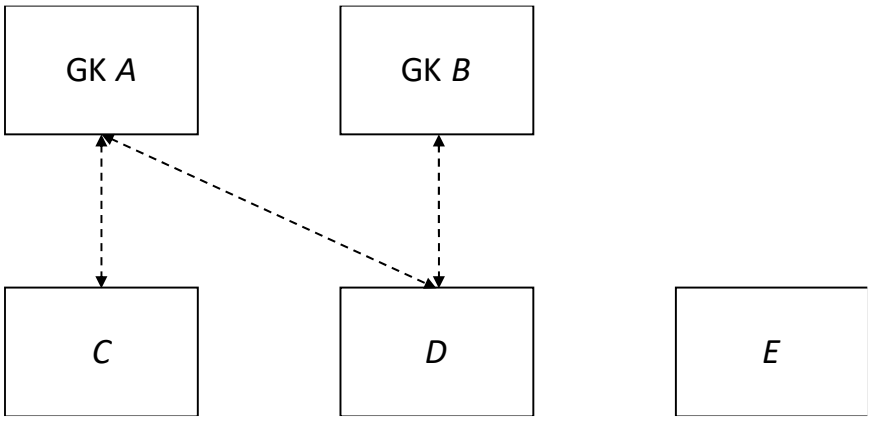


Figure 2: Example 2: third party C is interoperable with gatekeeper A, third party D with A and B, and third party E with no gatekeeper.

These two examples show that **there are scenarios where group chats will not work effectively if users opt in to discoverability. Thus, one could argue for making user discoverability the default (and thus adopting the opt-out regime). However, this does not seem feasible to us for privacy reasons, as explained above, nor is it desirable to maintain transparency for users.**

3.2. Design of Interfaces

Implementing interoperability also requires new interface design, both for the gatekeepers and for the third parties who will request and use interoperability. And, as Blessing & Anderson (2023) note, "[i]Interface design is critical if messaging interoperability is to enhance, rather than degrade, the user experience."

There is a concern that gatekeepers might choose a bad design to make interoperability ineffective. This is related to the more general issue of choice architecture, which is discussed in more detailed in another CERRE paper.[70] We discuss here two specific topics that raise design concerns: (i) the choice of communication channel; and (ii) possible alerts to users for interoperable communications.

3.2.1. Choice of communication channel

Let's say Alice wants to communicate with Bob. Since they use different messaging services, this communication is done through interoperability. However, Bob uses multiple messaging services, all of which are interoperable with Alice. In this case, who should decide which service to use to terminate the communication on Bob's side?

If Alice is the one making the decision, there should be an interface in her application to select which service to use on Bob's side. The figure below shows an example of a possible design from Matrix.

[70] See Fletcher, A. (2023), "Choice Architecture for End Users in the DMA," CERRE Issue Paper.

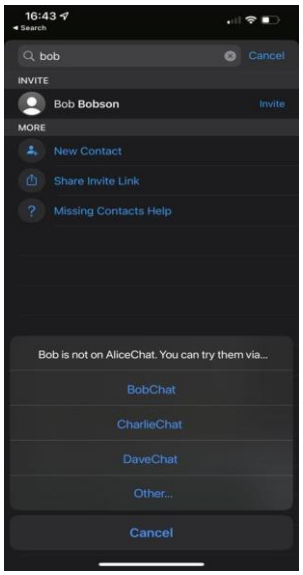


Figure 3: Alice wants to communicate with Bob. She is using AliceChat (a gatekeeper app). She is prompted to choose a service that Bob uses. Source: https://matrix.org/blog/2022/03/29/how-do-you-implement-interoperability-in-a-dma-world/

Alternatively, we could argue that it is up to Bob to decide. In this case, there should be an interface where Bob specifies his preferred service to receive interoperable communications. Should it be the same for every contact? Or will Bob be able to fine-tune it by selecting an interoperable channel for each contact?

Finally, the preferences of both the initiator of the communication (Alice) and the destination (Bob) could be taken into account to select the communication channel. For example, Alice and Bob could rank their preferred services and an algorithm could select the best service for them based on a decision rule. However, such a solution could be complicated to implement in practice.

To the extent that Bob has given his consent to communicate with Alice, we would tend to argue that the solution to this problem is not critical. So **there could be a default to avoid users having to make this choice for every call, with the possibility for users (Alice and/or Bob) to override the default if they wish**.

3.2.2. Alerts to users for interoperable communications

Interoperability may involve privacy or security trade-offs (see our discussion of these trade-offs in Section 4.2). When a user is about to make an interoperable communication, should the user be warned of the possible negative privacy or security consequences? Matthew Hodgson of Matrix argues that "unless everyone speaks the same end-to-end encrypted protocol", the user should be warned that "the conversation is no longer end-to-end encrypted", for reasons of "user experience and transparency" (see the example below).[71]

[71] See the blogpost https://matrix.org/blog/2022/03/29/how-do-you-implement-interoperability-in-a-dma-world/.

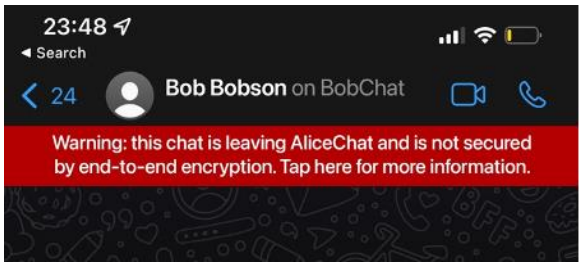


Figure 4: Alice wants to communicate with Bob. Alice is on AliceChat, but Bob is on BobChat, so she will make an interoperable communication. She is warned that this communication will not necessarily be as secure as on AliceChat. Source: https://matrix.org/blog/2022/03/29/how-do-you-implement-interoperability-in-a-dma-world/

However, such alerts or warnings could be frightening to users and discourage them from interoperable communications. One solution could be to ask users to consent to an interoperable communication with another user when it is about to be established, as we discussed above. The need for such alerts also depends on how strict the screening of interoperable providers is. If only providers that meet certain security standards can become interoperable, security alerts may not be necessary.

In any case, **careful design of these interfaces will be necessary** for interoperability to be effective.

4. TECHNICAL CHALLENGES AND TRADE-OFFS IN IMPLEMENTING HORIZONTAL INTEROPERABILITY

Next to implementation challenges with respect to consent management and re-designing the interface of NI-ICS so that interoperability becomes seamless for users, there are also a number of technical challenges and trade-offs that need to be considered and resolved in order to make interoperable end-to-end-encrypted messenger applications a reality.

Indeed, in mandating interoperability between existing NI-ICS, the DMA poses new technical questions for which solutions are not available off-the-shelf. The main reason is that the DMA requires gatekeepers to make messaging apps interoperable that have not been designed with interoperability in mind. While there may exist protocols for a federated, interoperable messaging infrastructure, such as the Matrix protocol,[72] the use of such a protocol requires that every gatekeeper (and every competitor seeking interoperability) updates its current implementation and adopts the standardised federated protocol from here on for off-net communication. Moreover, the Matrix protocol has its own set of security concerns (see, e.g., Albrecht et al., 2023). For on-net communication the proprietary protocol could be maintained (see also Section 4).

Federation of messengers works in similar ways as eMail. Users can choose one of many service providers that run independent servers, but all providers need to implement the same federated protocol (e.g., Matrix in case of messengers, or SMTP in case of eMail), so that the different servers can exchange messages. Federation is also the preferred solution to interoperability by many technologists, such as the newly founded workgroup on More Instant Messenger Interoperability (MIMI) by the Internet Engineering Task Force (IETF), the standard setting body for Internet protocols. However, federation and adoption of a common protocol goes well beyond what is demanded by the DMA, which only requires in Article 7(1) that a gatekeeper "shall make the basic functionalities of its number-independent interpersonal communications services interoperable with the number-independent interpersonal communications services of another provider, [] *by providing the necessary technical interfaces or similar solutions that facilitate interoperability."*

The challenge of making secure messenger apps interoperable *ex-post* into existing systems is thus very different from designing a federated secure infrastructure of interoperable messengers *ex-ante* (from scratch). Due to the unique challenge posed by the DMA to open up closed messengers ex-post, technologists have just begun to think about possible solutions and – from a technical perspective – there is a lively debate and no silver bullet solution that would necessarily win the race. In addition, Article 7(4) makes clear that it is upon the gatekeepers and not the Commission or third parties (e.g., firms wishing to request interoperability) to propose a technical solution ("reference offer laying down the technical details and conditions of interoperability"), and gatekeepers may not have the same incentives as the Commission or an independent third party when it comes to implementation options.

[72] https://en.wikipedia.org/wiki/Matrix_(protocol)

As with every technological design, there are many small and large trade-offs that need to be navigated when designing new protocols or interfaces, and non-technical trade-offs (such as governance or transparency issues) can be factored into the design. In effect, this can make a specific interoperability implementation more or less attractive to competitors. Moreover, the effectiveness of the specific interoperability implementation may not even depend on the gatekeeper alone, but also on which competitors precisely seek interoperability and which pre-existing technical designs and business models they pursue. For example, designs that minimise the exchange of metadata (or more generally designs that lean towards user privacy) are likely to lead to less user convenience and are less preferred by firms that seek to run an advertising-based business model. Against this backdrop, **there is no 'gold standard' against which the Commission may judge the gatekeepers' implementation proposals**.

Nevertheless, it is useful to briefly discuss the main technical trade-offs that should be considered when evaluating specific implementation proposals. Len et al., (2023) see three main areas that need to be considered (and agreed on) when designing interoperability ex-post:

1. *Identity interoperability*, i.e., how users can be discovered on other networks;
2. *Protocol interoperability*, i.e., how a secure channel can be established for cross-network communication;
3. *Abuse prevention*, i.e., how networks can and are allowed to deal with malicious actors (e.g., spammers).

We describe each in more detail below. We thereby focus on the simplest case where text messages are to be exchanged between two parties (sender and receiver). This is also the first step that is required by the DMA. In subsequent steps, interoperable group chats and voice communication are required. These present additional challenges and the complexity is likely to rise significantly. This is because communication is n:n in group chats (as opposed to 1:1 communication in two-party exchange) and each sender/receiver may reside on a different network, using a different identity service and protocol. In voice communication, the main additional challenge lies mainly in achieving encryption in a synchronous manner and on-the-fly, which presents additional requirements on hardware and software.

4.1. How to Resolve Identities across Providers

In a centralised non-interoperable system, identity management is a relatively straightforward task, as there is only one central authority that grants user identities. The central authority can make sure that the namespace is well qualified and identities are unique. Users need to trust that their provider verifies identities correctly, so that they are really communicating with whoever they think they are communicating. But users only need to trust their provider.

This is **not necessarily the case in a decentralised, interoperable system, where different entities can grant identities**. Here users need to trust all providers, and there is no guarantee that the namespace is unique and well qualified.

Generally, an **identity involves at least two parts: a common identifier (e.g., a username) and a public key (the cryptographic identity)**. Different NI-ICS use different types of identifiers. Although NI-ICS are "number independent" (which means they do not rely on the public telephone system), they often use mobile telephone numbers as identifiers. However, other NI-ICS use self-selected usernames, email addresses or random numbers as identifiers. Identifiers can or cannot tie to real world identities, which already presents a trade-off between privacy and security that different providers strike differently.

The public key is one part of a public-private key pair, which is needed to establish a secure connection. Simply put, a sender retrieves the public key belonging to a certain receiver and uses that key to encrypt the message. The message can then only be decrypted using the private (secret) key of the recipient (and the public key of the sender). Therefore, the issue of identity interoperability generally involves two subtasks. First, **identity discovery**, i.e., making identifiers established and authorised by one provider known to the other providers). This also involves learning at which other provider the designated target identity resides. Second, **retrieving the public key** belonging to a specific identity, which is then the prerequisite for initialising a secure connection. While each part bears its own challenges (cp. Len et al., 2023, Blessing & Anderson 2023), we focus on the issue of identity discovery here.

Several different implementation options exist to address the identity discovery problem. According to Rescorla (2022a), they can be roughly categorised in those solutions that strive to achieve a globally unique namespace, which ensures that every identifier exists only once globally, and solutions which allow for non-unique identifiers ("unqualified namespace"). Each approach has advantages and disadvantages.

The advantage of an **unqualified namespace** is that each provider in an interoperable system can continue to use whatever identifiers it is currently using (telephone numbers, random numbers, etc.) irrespective of whether the identifiers is globally unique. In reverse, this approach requires some kind of centralised look up service, which delivers all matches to a given identity search. Users would then pick the appropriate identity from a list (e.g., annotated with some metadata such as location or provider of the user for disambiguation). Such a look up service can pose some risks to privacy (Rescorla 2022b, Len et al., 2023) and no readily available (standardised) solution seems to exist today that is suitable for the specific case of messenger interoperability (Rescorla 2022b), albeit some solutions (like SPIN[73]) have been proposed.

A **globally unique namespace** can be achieved either using a hierarchical approach or a centralised approach. The hierarchical approach is commonly used in federated systems, such as Matrix, eMail or the Domain Name System (DNS). It means that the global namespace is divided into different subspaces, controlled by different entities that ensure that their respective namespace is unique. For example, each eMail address is unique and split into two parts like identifier@server.com. The part behind the @ designates the entity that controls the subnamespace. This must be unique. The part before the @ is the identifier that is guaranteed to be unique only in the given subnamespace. The

[73] See https://www.ietf.org/archive/id/draft-rosenberg-dispatch-spin-00.html

same system can be used for interoperable messaging, where each pre-existing (possibly non-unique) identifier is annotated by a unique identifier for the specific provider. In the hierarchical approach, identity recovery is resolved through the respective server of the subnamespace. This can also have the advantage that no central server exists which has control over all identities, which bears advantages from a privacy point of view and is also more robust to certain types of attacks (e.g., denial of service attacks) than a centralised system. The disadvantage, however, is that identities are provided by several different entities, which need to be trusted. Furthermore, a unique namespace can also be established by relying on another unique namespace, such as mobile telephone numbers. While this may ensure that a number belongs to a certain person, the same mobile number could be registered with several NI-ICS providers. Thus, one would still have to discover at which providers the number is registered, i.e., another type of look up service is required. Finally, one could also establish a centralised database, where each provider is required to register its identities, and which makes sure that the identifiers are unique. This would also require, however, that already existing non-unique identifiers of various providers would have to be resolved somehow, i.e., some users may not be able to keep their existing identifier. It also bears the question who should operate the central database, which would be crucial for the functioning of interoperability across various providers.

The previous derivations already highlight that the problem of identity discovery is non-trivial when interoperability is imposed ex-post. Most importantly, however, the preceding discussion highlights that **no matter which approach is chosen, some standardisation/agreement between providers is required**. Moreover, either **each provider must be trusted** that it has appropriately verified the identity of the user using some external identity (e.g., by sending a SMS to verify a phone number) or all providers need to trust a central authority to do so. End-to-end encryption is essentially meaningless if the end points of the communication (the identities) are not sufficiently validated (Blessing & Anderson 2023).

4.2. How to Establish Secure Connections

Today many prominent messaging apps employ some kind of end-to-end encryption (E2EE) at least for basic text messages. This means that the communication is secured (to various degrees) between two trusted end points of the communication. End points are typically the hand held devices of participants. Thus, it is important to note that “security” relates only to the communications channel and parties need to trust that the end points are secure and not compromised. Actors having control over the end point (e.g., the operating system, the messaging app itself, or if third parties can access to the smartphone) could theoretically eavesdrop on the communication or establish backdoors without compromising E2EE as such.

Different messaging services typically use different (incompatible) protocols for E2EE. Figure 5 shows an overview of the different protocols used for popular messengers presented in Wiewiorra et al (2022). The figure is already a bit dated by now, as some of the messengers have since added support for E2EE (in group chats), or changed the protocol that they use for encryption. However, the main message of this figure is that the protocols implemented in popular messaging apps are diverse and subject to constant evolution. In a more detailed analysis, Rösner & Schwenk (2023) conclude that difference between protocols are “so manifold and diverse that an attempt to provide interoperable

messaging by converging the current protocols is pointless." Albeit several messengers use Signal's Double Ratchet protocol, and some use derivations of that protocol, the implementations are not directly compatible or interoperable (Blessing & Anderson 2023). It is also important to note that different E2EE protocols imply different security levels (cp. Rösner & Schwenk 2023). In this context, it is noteworthy that some use open source protocols whereas others (including WhatsApp and iMessage) use proprietary protocols. Open source protocols can be verified by independent third parties, as the source code is open; on the contrary this is not the case for proprietary protocols. Thus, the actual level of security is often not known publicly. Further, there is much more to security than just the naked E2EE protocol. For example, some providers may use forward secrecy (a feature that creates temporary keys in order to protect past communication in case an end point has been compromised) whereas others do not. Some providers may rotate the keys more frequently than others, verify user identities more stringently, and so on. Generally, the more secure E2EE is, the more difficult is it to preserve the same level of security when more providers are involved in the communication (Blessing & Anderson 2023).

Service	End-to-end encryption bilateral:	End-to-end encryption group:
Discord	N	N
Element (Matrix)	Olm (Signal-based)	Megolm (Signal-based)
FB Messenger	Proprietary (Signal-based)	N
Google Chat (Hangouts)	N	N
iMessage	Proprietary	Proprietary
Instagram DM	Proprietary (Signal-based)	N
Kik	N	N
Signal	Signal protocol	Signal protocol
Skype	Proprietary (Signal-based)	N
Slack	N	N
SMS (trad. TC)	*N*	*N*
Snapchat	N (Images only)	N
Telegram	Proprietary (MTProto 2.0)	N
Threema	NaCl	NaCl
Viber	Proprietary	Proprietary
WeChat	N	N
WhatsApp	Proprietary (Signal-based)	Proprietary (Signal-based)
wickr	Proprietary (source code visible)	Proprietary (source code visible)
Wire	Proteus (Signal-based)	Proteus (Signal-based)

Figure 5: Different end-to-end encryption standards used in different popular messengers according to Wiewiorra et al., (2022). "N" denotes that messages are not end-to-end encrypted. Figure is meant to reflect mere the diversity of protocols used at a given point in time. Figure reflects the state in 2021 and does not provide a complete overview over all messaging services. Changes and updates have occurred since then, reflecting the fast technological progress in the messaging space.

Also note that **E2EE of group chats is considerably more complex**, and thus less commonly employed in many messengers. Group chats between n parties are often emulated by sending n-1 bilateral messages, which creates significant message overhead. In addition, there need to be protocols to securely and efficiently add and remove group members, which remains an active area of research (Len et al., 2023). A promising candidate E2EE encryption protocol for secure group chat messaging is Messaging Layer Security (MLS), which has in March 2023 been approved by the Internet Engineering Taskforce (IETF) as a new standard. The standard is backed by some major messaging app providers (e.g., Wire and Google).

In any case, given the myriad of different and incompatible E2EE standards, in order to achieve interoperability there are only two options:

1) The sending provider and the receiving provider would need to agree on a **common encryption protocol** (e.g., one party adopting the protocol of the other). This may also mean that all providers implement all protocols of the other providers, and use whichever protocol is necessary in a given communications scenario.

2) Either the sender or the receiver, or both need to do support multiple protocols and there is some **translation from one protocol** to the other when sending or receiving messages across different protocols.

Interestingly, in Article 7(3) the DMA explicitly demands that E2EE is preserved by interoperability. This seems to rule out scenarios in which there is a server-side translation (so-called "**server-side bridge**"). In this case, the end point of the secure communication would be a central server (the bridge), which decrypts the message coming from the sender, using the sender's encryption protocol, and decrypts the message again using the receiver's encryption protocol. However, this implies that the message is intermittently not encrypted – which breaks the notion of E2EE.

If the translation is done at the end point (e.g., a user's smartphone), however, then this would not break E2EE, as translation is done at the end-point (rather than an intermittent server). Therefore, such a **client-side bridge** is an option that has gained some attraction, as E2EE can be preserved, and each provider could largely keep their existing E2EE implementations (Blessing & Anderson 2023). The major flip side of this approach is that with each new provider joining the circle of interoperable providers, all other providers have to update their clients and implement that providers protocol as well. The implementation cost and complexity of this may be insurmountable especially for small provider – who are the intended beneficiaries of interoperability. Moreover, there is additional burden on the end user device, and this makes the end user software more complex (and likely more vulnerable to attacks).

This also relates also to another major design decision when implementing protocol interoperability ex post, i.e., whether a client-to-server framework or server-to-server framework is adopted (see Figure 6).

In a **client-to-server framework** the gatekeeper's server (say receiving a message) allows alternative clients (say sending a message) to connect, possibly in similar ways as the gatekeeper's native clients would connect to the server. Thus, only one server is involved in the end-to-end-communication. Since the receiver's/gatekeeper's provider and the sender's/competitor's provider very likely use different protocols for end-to-end-encryption, the competitor's client would need to implement different protocols for communicating with its own server and that of the competitor and – depending on which server it communicates with – use the appropriate protocol. This approach requires major updates in the client apps of non-gatekeepers and tends to make end user apps more complex, i.e., more error prone and larger in size. This approach seems to be the less favoured approach currently by independent experts, such as the IETF MIMI working group.

In a **server-to-server framework**, the gatekeeper's server and the competitor's service exchange the messages directly, and the competitor's clients just communicate with the competitor's server. This means the competitor's app does not have to undergo significant changes. In the server-to-server framework both servers are in involved in the end-to-end-communication. From a top-down perspective, the server-to-server framework seems to be the more attractive choice (Len et al., 2023), as implementation costs are lower for competitors. There may even be some additional advantages with respect to privacy, as each server could act as a privacy relay with respect to its connected users, so that no single server has full knowledge over the social graph (which is an inevitable outcome if there is only one server involved). However, from the perspective of gatekeepers, who are the ones

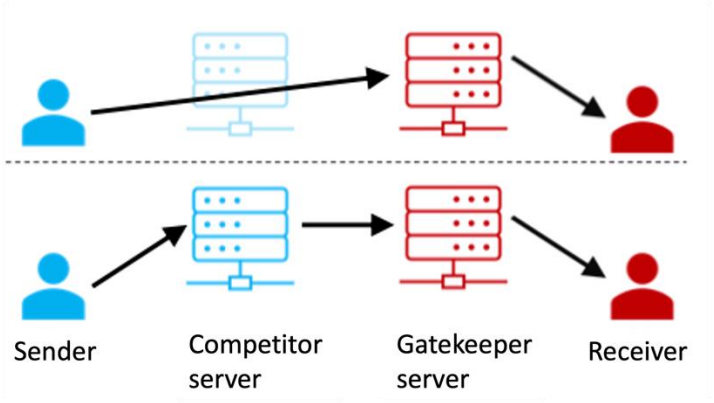


Figure: Interoperability can be implemented in a client-to-server framework (top) or a server-to-server framework (bottom).

making a proposal on how to implement interoperability, the client-to-server framework could be more attractive (possibly for the same reasons).

4.3. How to Take Action against Malicious Users

Abuse prevention is arguably a significant area that contributes to the "integrity, security and privacy" of a NI-ICS, and as such it is relevant in the context of Article 7(9), which allows gatekeepers to take strictly necessary and proportionate measures to protect these very values.

Abuse prevention is already a challenge for centralised messaging services. This challenge is **significantly amplified in an interoperable system, because there is no central authority** that can enforce abuse across all users. A common technique to prevent abuse is content moderation, either through algorithms or through humans, or a combination of both. However, when the message content is end-to-end encrypted – as is common among popular NI-ICS – classic content moderation is not an option. The remaining options are to rely on user reporting (so abusers can be blocked centrally), blacklisting (allowing users individually to block certain users) or to use metadata (e.g., who has communicated with whom, how many messages have been sent, timestamps, length of messages) to detect abusive behaviour. All of these measures are typically employed by popular NI-ICS, and in light of Article 7(9) the question arises how they could be preserved in the context of interoperability.

User reporting is considered an effective method for countering abuse at scale (Blessing & Anderson 2023) and is therefore a very popular method employed (Len et al., 2023). When users report abuse, their client typically gathers information about the reported user, such as the user's identity, the reported message, but also a number of previous messages to provide context, and sends it to the central authority. This is also the approach taken in WhatsApp and iMessage (Blessing & Anderson 2023, Len et al., 2023). Providers also employ *message franking* in order to prevent users from providing false abuse reports. Such message franking would also need to be made interoperable, which presents a challenge (Blessing & Anderson 2023).

While user reporting relies on a review by the provider, **blacklisting is an immediate action that a user can take in order not to receive further messages from an abusive user**. It as well is frequently employed in E2EE messengers. However, interoperability requires that users would also be able to blacklist users of other providers, which presents another challenge. In particular, an abusive user may have accounts with several other providers, and in order to be effective across networks, blacklisting would need to be propagated to all those providers at which the abusive user has an account. Also blocked users (either by user reporting or blacklisting) may just make new accounts, either with the same or with new (interoperable) providers. The costs of getting a new identity at a pre-existing provider can be relatively high (e.g., requiring a new telephone number) depending on whether or not the identity is attached to some external identity that is verified by the provider (see Section 3.1). Instead, obtaining a new identity at a new provider can be of substantially lower costs, e.g., because the new provider does not require an external identity such as a telephone number. This means, with interoperability also those providers at which the abusive users does not yet have an account may need to be notified in order to prevent these so-called sybil attacks.

Both blacklisting and user reporting are retroactive measures. By contrast **abuse detection based on metadata (e.g., spam filtering) is a proactive measure**, which also is frequently employed by messaging providers. Albeit the message content itself is not accessible due to E2EE, metadata is typically not encrypted (and to some extent cannot be encrypted). Metadata is collected and stored to various degrees by different providers, and can involve a user's social graph (which identities have communicated with each other, contact lists, etc.), location data, time stamps of (encrypted) messages sent, filetypes sent, and so on. More privacy affine messengers tend to collect less metadata. But there is a trade-off, as more metadata (e.g., the frequency of messages sent by a given user) also helps to detect abuse. In a centralised system, metadata is collected by one provider, which also facilitates abuse detection. In a decentralised, interoperable system, no single provider likely has all metadata. In fact, (sever-to-server) interoperability can be implemented such that it acts as a privacy relay and prevents the spreading of metadata to other providers (Len et al., 2023). However, this also makes abuse detection and prevention more difficult. Even worse, this may even lead to a rise in abusive behaviour, as the moral hazard increases due to the lower detection probability. Further, similar as in the case of blacklisting, effective spam filtering probably requires a shared perception over some metadata, e.g., to impose inter-provider rate limits on forwarded messages in order to prevent the spreading of viral message (Blessing & Anderson 2023).

It is also worth mentioning that **the trade-off between privacy and detection probability, as well as the implementation of spam filtering is likely to differ between text messages and voice calls**. While

text messages could be delayed (for the provider to review, e.g., with respect to metadata), or put in a separate folder (for the user to review), this is not an option for voice calls. This in turn may have an impact on the privacy-detection balance that providers need to navigate, and that they need to find some common ground on when systems are interoperable.

5. TRADE-OFFS

Against the backdrop of the preceding section, we now highlight some of the main trade-offs involved when implementing Article 7 of the DMA more explicitly, and also point to open questions that need to be considered. We focus on one-to-one messaging, as the interoperability obligation will initially apply only to this context, and only later on extend to group messaging.

5.1. Interoperability Implementation Trade-offs: APIs vs. Standardisation

One main trade-off is between standardisation (which requires all interoperable messengers to implement the same standardised cryptographic API for interoperability) and the use of proprietary APIs (where interoperability is established through the implementation of the various cryptographic APIs of the other providers). In the latter case, we can differentiate between a gatekeeper-side API approach (where the gatekeeper implements the APIs of the competitors seeking access) or the competitor-side API approach (where the competitors implement the APIs of the gatekeeper or gatekeepers).

Rösler and Schwenk (2023) go through the pros and cons of these approaches in some depth and come to the conclusion that **only the competitor-side API is realistic**. A standardisation approach would require all firms to agree on a common standard, which takes time and involves uncertainty. All firms would then have to implement the new standard, which could possibly lower the security standard for some, and increase the security standard for others. For example, some protocols implement forward secrecy, whereas others do not. Importantly, firms could yet keep their proprietary protocols for on-net communication. The standardised protocol would only be needed for off-net communication. Nevertheless, standardisation is a lengthy process, and it is unrealistic that it can be completed in due time. Furthermore, gatekeepers may not have an incentive to conclude that process successfully.

However, **in the long run, especially if there is more than one gatekeeper[74] to be designated under Article 7, standardisation is arguably the best option** from a technological point of view, as it does not create a patchwork of APIs like the other approaches.[75] With a standardised API, all firms would just need to implement one API. With the other approaches, one API per gatekeeper (or competitor) needs to be implemented. We note that Article 48 (see also Recital 96) enables the Commission to task a European standardisation body to develop an appropriate standard to facilitate interoperability. As we have pointed out above, there are at **least three areas in which standardisation may be necessary (discoverability, secure messaging and abuse prevention).** On the other hand, the DMA is clear in Article 7(4) that the gatekeeper has to provide a technical reference offer first. By Recital 64, the Commission can consult BEREC (which is not a standardisation body, however) whether the

[74] At the time of writing, WhatsApp and Facebook Messenger are designated as core platform services. The designation of iMessage is still under investigation.

[75] Also, the patchwork of APIs seems unworkable for group messaging involving more than two providers.

reference offer is compliant. It is unclear, however, at which point exactly the Commission can demand a standardisation process according to Article 48.

Gatekeeper-side API would require the competitors to expose an API, which would be implemented by the gatekeeper to send and receive message to and from the respective competitor. This would put the implementation effort mainly on the gatekeeper, which probably has the resources for doing so. However, it would probably be the least preferred option by the gatekeeper, as it has to bear the implementation effort and would be dependent on the APIs provided by competitors.

In reverse, the **competitor-side API** approach requires the competitors to implement the gatekeeper's API; and if there are several NI-ICS core platform services, competitors would need to implement several APIs. The implementation burden would be rather on the side of the competitors. Rösner and Schwenk (2023) differentiate between two instances of the competitor-side API approach. In the first, so-called **competitor-implemented** approach, the gatekeeper would need to specify its cryptographic protocol in sufficient detail, so that it can be implemented by competitors. This poses the biggest implementation effort for competitors, but as a positive side-effect it would de-facto open source the hitherto proprietary cryptographic protocol, which allows for an independent assessment of its security level. The cost of implementation of the competitor-implemented approach can be high, however. The alternative is the **gatekeeper-implemented** approach, where the gatekeeper would provide (closed source) programming libraries to the competitors. The competitors would need to implement those libraries in order to encrypt or decrypt messages to and from the gatekeeper. The cost of implementation for competitors are significantly lower in this case.

The **competitor-side gatekeeper-implemented approach seems to be the most obvious choice** from a gatekeeper perspective. However, it also means that the gatekeeper keeps considerable control over the communication process, as competitors are fully reliant on the gatekeeper's library. In this approach, the level of security cannot be verified by competitors. They need to run executable code of the gatekeeper, and thus also need to trust the gatekeeper's library in that it does what it is supposed to do, and not more.

Importantly, the preceding discussion on standardisation primarily deals with protocol interoperability as presented in Section 3.2. Even if a competitor-side gatekeeper-implemented approach is adopted (which involves no standardisation per se), some standardisation would reasonably be needed to address the issue of identity interoperability (i.e., to publish client identities and to distribute cryptographic keys), as discussed in Section 3.1 (see also Rösler & Schwenk 2023). This is particularly the case when there is more than one gatekeeper service. Additional standardisation is likely needed for interoperable abuse prevention (see Section 3.3). The DMA does not formally require any form of standardisation, however.

From this discussion **several questions emerge for the implementation** of Article 7:

- Given the benefits of standardisation for an effective implementation, how much can the Commission push for a standardisation approach with respect to i) identity interoperability, ii) protocol interoperability, and iii) abuse prevention? At which point can it invoke Article 48?
- In case a standardisation approach is pursued, should the Commission just relegate the standard setting process to a standard setting body or govern the process more closely in order to ensure that interests of gatekeepers and access seekers are well balanced in the standardisation outcome.[76]
- Under Article 7(6) can additional time be granted before gatekeepers need to be compliant in case they opt for a standardisation process, as it is not realistic to complete the standardisation process within 6 months.
- Under which conditions can the standards be changed (by the gatekeeper or competitors)? Can the Commission invoke Article 48 again to change a standard that has been set previously using Article 48?
- Some gatekeepers may be designated later. In case a standard exists by then, can they be bound to use it? Or can they make a non-standard compliant reference offer?

5.2. Implications of Interoperability on Security vs. Privacy Trade-offs

A second major trade-off in the design of any NI-ICS, but especially interoperable NI-ICS, relates to the **trade-off between privacy and security**. The conflict arises, because E2EE is meaningless if the end points of the communication are not verified for authenticity. As we have discussed in Section 3.1, this often involves verification of user identity through external identifiers (such as phone numbers).

Trade-offs between privacy and security also arise in the context of abuse prevention, as discussed in Section 3.3. Abuse prevention is more effective if metadata is shared among providers, possibly even with providers at which a user does not (yet) have an account in order to prevent sybil attacks. Article 7(8) demands that not only such personal data is shared as is "strictly necessary to provide effective interoperability"? However, Article 7(3) demands that the "level of security" shall be preserved across the interoperable services. **These two provisions may likely be at odds**, as different providers establish different levels of security also by collecting different amounts of metadata that facilitate abuse prevention. As discussed in Section 3.3, there is a need to share metadata for effective abuse prevention, which falls under the umbrella of a system's "security".

Len et al., (2023) propose that the sender's provider should be responsible for abuse detection based on metadata and filter out messages before they are relayed to another provider. This, however, means that providers would have to rely on an external (competing) provider for abuse detection (Blessing & Anderson 2023), which is probably not acceptable for many providers, and also gives rise to issues of moral hazard. This also does not resolve the issue that generally less metadata is available

[76] Political involvement in standard setting processes is not unusual and was, for example, also the case in the development of the GSM standard for mobile communications.

(compared to a central system) on which the detection can be based, which likely lowers the detection rate.

More generally, from our discussion in Section 3 it is **difficult to see how interoperability would not affect the level of security or privacy in one way or another**. We acknowledge that there may be some isolated instances and implementation in which privacy or security is indeed improved through interoperability. For example, because in a server-to-server framework, each server can act as a privacy relay (Len et al., 2023). Or because interoperability requires some clients to adopt more secure protocols (Blessing & Anderson 2023). However, in general interoperability requires to increase the circle of trusted parties, requires to share some (meta-)data across several providers and increases protocol complexity. All of this increases the possible threat vectors and tends to lower the overall level of security (Blessing & Anderson 2023), even if at a cryptographic level the level of security is maintained. In this context, some privacy-focused messengers such as Threema and Signal have already announced publicly that they do not want to seek interoperability under the DMA because of security and privacy reasons. In reverse, Articles 7(3), 7(8) and 7(9) may therefore be powerful defenses for gatekeepers objecting interoperability.

From this discussion **further implementation questions arise**, such as:

- Is a gatekeeper allowed to reject an interoperability request if the competitor's service does not verify a users' identity based on some external identity? Otherwise, the "level of security" may be lessened.
- How will a gatekeeper verify the level of security of a competitor's service (e.g., using a proprietary protocol)? Will they have to take their word for it? Do they have authority to demand critical information? Can they turn to the Commission to verify the level of security and/or to obtain critical information? For example, if the competitor's service is closed-source, will they have a right to obtain the competitor's source code? Under what conditions can they refuse an interoperability request based on protocol security?
- Can gatekeepers deny interoperability with messengers that do not employ appropriate abuse prevention or cooperate in abuse prevention, e.g., by sharing data about the reported user?
- How much metadata would other services need to share with a gatekeeper, and vice versa, to maintain the same "level of security"? Can gatekeepers refuse an interoperability request if not sufficient metadata is shared?
- Under what conditions can a gatekeeper refuse to trust a third party?

5.3. Interoperability vs. Usability Trade-offs

Interoperability also involves unique trade-offs for usability and the design of user interfaces. First, there is a **trade-off between usability and privacy/security that different providers strike differently**. For example, a privacy-affine messenger like Threema does not use phone numbers as identifiers, which arguably has downsides for usability. As discussed in Section 3.1, interoperability requires some identity interoperability which can interfere with that trade-off and likely has a negative impact on

usability. Similar trade-offs arise with respect to usability and security. Some messengers change cryptographic keys more frequently than others, but as discussed in Section 3.2, protocol interoperability requires to adopt a scheme that is compatible with the gatekeeper.

Interoperability also has implications for the user interface design. This involves the **discovery process of other users on other messengers**: How many other providers are visible to a user? Can a user choose on which other providers he or she wants to be discoverable? How many "search results" does the discovery service provide? It is evident that such design decisions can have significant implications to which interoperability is perceived useful by end users, and thus to which extent interoperability may facilitate market contestability.

As interoperability is only required in the EU, a question also arises **which users are discoverable across messengers. Only users from the EU, or all users?** Especially if discoverability requires changes in the namespace (see Section 3.1), users outside of the EU are likely to be affected by system-wide changes one way or another.

Interoperability may also require to **distinguish between messages coming from alternative providers**. However, dark patterns could be used to discourage interoperability, for example, by coloring interoperable communications in a certain way to make them look "bad" (Blessing & Anderson 2023).

The interface design also needs to account for the more complex **consent management**, as users can opt out of interoperability by Article 7(7). As the list of interoperable competitors grows, this can have significant implications on usability, especially in the context of group chats. Here, likewise dark patterns may be employed.

5.4. Interoperability vs. Innovation

Interoperability can also affect innovation efforts. In Bourreau et al., (2022) we discuss this complex issue in detail and more nuanced, whereas we can only provide a synopsis of the main arguments here. **Some have argued that interoperability can spur innovation** (Scott-Morton et al., 2021), because interoperability is limited to basic functionalities. Post interoperability of basic functionalities, providers seek to differentiate themselves through new non-interoperable features to attract consumers. However, if this is the case, and consumers indeed see value in those new features, it also undermines the value of interoperability, as important (future) features are not interoperable.

In reverse, interoperability can also undermine innovation efforts when such features are meant to be interoperable. Blessing and Anderson (2023) provide the example of self-exploding messages that are automatically deleted after some time period. If such a feature were to be made interoperable, then first, different providers need to agree on a common form (e.g., acceptable time limits) for those new features, which slows down the innovation process. Second, providers need to rely on and trust other providers that messages are indeed deleted as specified. Users also need to trust that this is indeed the case across providers in order to be able to value this feature.

In case standardised APIs are used to establish interoperability (and to some extent also in the case of a gatekeeper-side competitor-implemented approach), it becomes more difficult to change the

standard, as it involves a collective action by all parties involved. This as well can stifle innovation. To be fair, technical standards can allow for some degree of extensibility (such as in the case of XMPP – the Extensible Messaging and Presence Protocol), which alleviates some of these concerns. However, the argument remains that innovation is more constrained, as it still needs to respect the limits of extensibility and possibly needs to maintain backward compatibility.

In reverse, as Figure 5 shows, competition between messengers (not adhering to a common standard) has led to several innovations and implementations in the cryptographic protocols. Different messengers strike the balance between usability, privacy and security differently. Importantly, as pointed out in Section 4.1, a standardised API may only be necessary for off-net communication, and providers could maintain differentiated protocols for on-net communication. Thus, providers would still be free to innovate with respect to their proprietary protocols (Rösner & Schwenk 2023). However, this as well would over time decrease the benefit of (off-net) interoperability, as the standardised API becomes frozen in time and does not keep up with the innovations that occur for on-net communication. The different innovation trajectory between on-net and off-net communication is amplified by the staggered implementation process of the Article 7 provisions, whereby interoperable functionalities only have to be implemented step-by-step over time. As a consequence, users are likely to perceive on-net communication superior to off-net communication, undermining the value of interoperability.

5.5. Interoperability vs. Multihoming

A final trade-off that we want to discuss here involves **messengers that facilitate multihoming, as an alternative to messengers that are interoperable**. As Len et al., (2023) point out, there already exist a few so-called multi-messengers that integrate several popular messaging apps (like WhatsApp and iMessage) under one combined user interface. These messengers include Beeper, Texts, and Mio. Little seems to be known about their implementation and level of security, but all seem to require that users have proper accounts on all messaging services that they want to communicate with.[77] Further, these messengers seem to rely on client-side bridging (cp. Section 3.2).

As we have pointed out in a previous CERRE report (Bourreau, Krämer & Buiten 2022), interoperability provides a partial substitute to multihoming. A user on a gatekeeper messenger that can communicate (even though only with basic features) with a user on an alternative provider does not need to make a proper user account with the alternative provider anymore. The user has less reasons to try out the alternative provider firsthand, and user experiences with that alternative provider are always mediated through the limited interoperable functionalities. In other words, interoperability lowers multihoming incentives, but multihoming can likewise be a powerful driver for market contestability. Users are thus also less inclined to use multi-messengers. To be clear, the DMA does not require any NI-ICS to take up an interoperability offer. So NI-ICS have an option to rather build on multihoming, or to build on interoperability. However, not all may be fully aware of the trade-offs involved.

[77] Some information about Mio's implementation and security-related aspects can be found in their white paper: https://go.m.io/security-white-paper

6. VERTICAL INTEROPERABILITY IN THE DMA

In this section, we build on our previous reports (Bourreau, Krämer & Buiten 2022, and Bourreau 2022) to discuss overarching principles that apply to the **main vertical interoperability obligations** introduced in the DMA:

- Sideloading of applications and app stores (Article 6(4));
- Access to essential hardware and software features of the operating system (Article 6(7)).

We refer the reader to these reports for a more extensive analysis.

It is inherent to vertical interoperability that the gatekeeper controls a bottleneck resource (e.g., the operating system) to which access is being provided. This is not necessarily the case for horizontal interoperability between NI-ICS, albeit – as we have shown above – this can be the outcome of specific implementations (such as the gatekeeper-side API approach).

Whereas the provision on horizontal interoperability is limited to the very specific case of NI-ICS, the provisions on vertical interoperability are potentially open ended and span over a much broader application scope, ranging from alternative app stores and applications to access to the NFC chip in order to enable alternative payment services. Nevertheless, **five overarching principles for implementation** can be highlighted (cf. also Bourreau, Krämer & Buiten 2022, and Bourreau 2022).

6.1. Screening of Access Requests

Article 6(7) DMA states that gatekeepers must provide “effective interoperability with (…) the same hardware and software features accessed or controlled via the operating system or virtual assistant (…) as are available to services or hardware provided by the gatekeeper.” Therefore, access to essential hardware and software features is mandated if the gatekeeper uses them for its own products or services, i.e., if it is vertically integrated.

In a previous report (Bourreau et al., 2022), we argued that vertical integration is a necessary but not a sufficient condition for mandating vertical interoperability. Indeed, it is well known that vertical integration also brings several efficiency benefits, such as the avoidance of double marginalisation and hold-up problems. Therefore, mandated vertical interoperability requires a clear theory of harm and justification.

The three-criteria test used in telecommunications regulation could be a possible approach, limiting mandated vertical interoperability to situations where i) there are high and non-transitory barriers to entry, ii) there is no trend towards effective competition, and iii) where competition law is considered insufficient. In particular, it should be **examined whether the hardware and software features are indeed "essential"**, i.e., whether they cannot be replicated by third parties, at least at a reasonable cost.

6.2. Screening of Access Seekers

Both, Articles 6(4) and 6(7) allow the gatekeeper to take strictly necessary and proportionate measures to protect the integrity and security of the gatekeeper's hardware and software systems. This can provide justification to **limit access only to those access seekers that meet certain security or integrity standards**. Note also that the screening of access seekers may be a substitute for notifying users of security or integrity risks - see our discussion of this trade-off below.

In addition, "free of charge" access may not send the right signal to access seekers, leading to (excessive) entry of possibly inefficient players. Therefore, the fact that access should be provided "free of charge" makes screening of access seekers particularly important.

One possible approach would be to **allow the gatekeeper to grant access licenses based on public, explicit and non-discriminatory criteria**. Under this access licensing approach, if the access is denied, the access seeker could appeal to the regulator. For access requests under Article 6(4), a fruitful starting point for a catalogue of security and integrity criteria is the "Code of practice for app store operators and app developers" developed by the UK Department for Science, Innovation and Technology.[78] Similarly, the gatekeeper should have the ability to revoke access licenses, again based on public, explicit and non-discriminatory criteria, for instance, if the access seeker does not comply *ex-post* with the requested security and integrity standards.

Another approach would be to confer the administration of the access regime to the **regulator or an independent third party**. For reasons of timeliness and pragmatism (the gatekeepers know their hardware and software and the associated risks best), we believe it makes sense to start with a gatekeeper-led approach in the beginning, and only turn to other solutions if that fails to achieve the desired goals.

Specifically, under Article 6(4), if alternative app stores are granted an access license, then these stores should also be responsible for screening the apps that they host. The screening process should comply to the responsibilities conferred under the license, but otherwise be independent of the gatekeeper's screening process.

It is also worth pointing out that **access conditions (based on security and integrity considerations) are likely to vary significantly depending on the specific functionality** that is to be made interoperable. This also means that the access conditions are likely to be different for those cases falling under Article 6(4) and those under Article 6(7).

[78] See https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

6.3. Gatekeeper-led Definition of Interfaces

Effective interoperability, or access to the hardware and software functions controlled by the gatekeeper, requires the definition of relevant hardware and software interfaces. An important question is who should define the interfaces?

We believe that the most appropriate approach is to allow the **gatekeeper to design and manage the interfaces**. From a technical point of view, the gatekeeper is in a better position to design the interface because it has developed the hardware or software technology. In addition, the platform can easily update the interface when technical changes are needed and can also take the necessary measures to ensure integrity and security.

However, there is a potential risk that the gatekeeper may use its dominant position to degrade the quality of the interfaces offered to some third parties. Access to these interfaces must therefore be **non-discriminatory**.

In the event of complaints and concerns about possible non-compliance, the regulator would investigate the technical specifications of the access interface.

An alternative approach would be to develop an **open interface standard**. The success of the Internet is largely attributed to its versatile open vertical interoperability standards (cp. the Open Systems Interconnection (OSI) model[79] for more details). However, the standardisation of interfaces can take a long time and it can be complex to reach consensus among market participants with different (and sometimes conflicting) incentives.

Note, however, that these two approaches are not necessarily exclusive. Interfaces based on proprietary interfaces could be developed in the short term, while a standardisation process could be initiated with the goal of developing open interfaces in the long term. Further, vertical access provisions under the DMA relate to proprietary platform services, for which it may not always be feasible to provide access through standardised interfaces.

6.4. Equivalence of Input

The general guiding principle for access to a particular hardware or software function should be the 'equivalence of input'; that is, an **entrant should have access to the same function, and on the same terms, as the vertically integrated gatekeeper for its own complementary products and services**.

Note, however, that "equivalence" does not mean "equality". Access to the hardware or software function may be provided through a specific API that is different from the internal API used by the gatekeeper, as long as the two APIs are "equivalent" in terms of functionality.

The 'equivalence of input' principle requires **monitoring to verify compliance** by the access provider, which can be complex and time-consuming. One possibility would be to have a first level of monitoring, where access providers would submit their process in their annual compliance reports. In

[79] See https://en.wikipedia.org/wiki/OSI_model for more details.

case of complaints from access seekers, more stringent forms of monitoring (e.g., through audits) could be introduced.

The gatekeeper could also gradually provide information on the software and hardware features that are accessible to third parties for access, with details of any restrictions for using them. An alternative to the 'equivalence of input' principle is an 'equivalence of output' principle. However, we strongly believe that whenever possible, 'equivalence of input' is to be preferred, as an access-seekers 'output' depends on various factors, many of which are not under the control of the access provider.

6.5. Neutral Choice Architecture

Since vertical interoperability implies that the gatekeeper is forced to open up a bottleneck resource (e.g., operating system) in order to enable alternative downstream providers (e.g., apps), the choice architecture for users for selecting alternative providers will be critical. Dark patterns in choice screens or self-preferencing would limit the ability for users to take advantage of the new alternatives and could therefore constitute a violation of the anti-circumvention clause in Article 13(6) DMA.

Therefore, open questions include what are acceptable choice architectures in the context of alternative distribution channels and what restrictions are absolutely necessary and proportionate for security reasons. The DMA provides some clarifications in Recitals 50-54. However, this remains a complex issue in its own, and it is dealt with in the companion issue paper on choice architecture.

Article 6(4) already provides explicit guidance on the choice architecture in demanding that third parties should be able to invite ("prompt") end users to set their app or app store as their default. Albeit Article 6(7) does not explicitly refer to a neutral choice architecture, the anti-circumvention clause in Article 13(6) DMA implies that the choices offered to end user should be presented in a neutral manner.

In all cases it should **be as easy for the consumers to install an alternative provider as it is for them to install the gatekeeper application** – without prejudice to the possibility to pre-install applications according to Recital 53 of the DMA. This can also be viewed and rationalised under the lens of equivalence of input (our fourth principle). Further, a neutral choice architecture also means that it is equally easy to change between alternative providers, as well as to change back to the gatekeeper. It may also involve prompting the user to reconsider their choices in reasonable intervals (see companion issue paper on choice architecture in relation to Article 6(4).

Finally, we wish to point out that there may be **interactions between the five principles that should be scrutinised by the Commission under the lens of proportionality**. For example, a gatekeeper may justify and employ a strict licensing regime, where it applies a certain security and integrity standard (yet, necessary and proportionate) when screening alternative providers before granting an access license. But in this case – in line with Recital 50 of the DMA – it does not seem "strictly necessary and proportionate" that the gatekeeper additionally presents warning messages to users whenever they seek to engage with one of the pre-vetted alternative providers. In reverse, when the gatekeeper pursues a very lenient access regime, or does no pre-vetting at all, then a warning message to users seems to be proportionate.

7. REFERENCES

Albrecht, M. R., Celi, S., Dowling, B., & Jones, D. (2023). Practically-exploitable cryptographic vulnerabilities in Matrix. Cryptology ePrint Archive, Paper 2023/485 Available at: https://eprint.iacr.org/2023/485.pdf

Blessing, J., & Anderson, R. (2023). One Protocol to Rule Them All? On Securing Interoperable Messaging. arXiv preprint arXiv:2303.14178. Available at https://arxiv.org/abs/2303.14178https://arxiv.org/abs/2303.14178

Bourreau, M. (2022). DMA Horizontal and Vertical Interoperability Obligations. Centre on Regulation in Europe (CERRE). Issue Paper. 11/2022. Available at: https://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdfhttps://cerre.eu/wp-content/uploads/2022/11/DMA_HorizontalandVerticalInteroperability.pdf

Bourreau, M., Krämer, J. & Buiten, M. (2022). Interoperability in Digital Markets. Centre on Regulation in Europe (CERRE) Policy Report, 03/2022. Available at https://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdfhttps://cerre.eu/wp-content/uploads/2022/03/220321_CERRE_Report_Interoperability-in-Digital-Markets_FINAL.pdf

Fletcher, A. (2023). Choice Architecture for end users in the DMA. Centre on Regulation in Europe (CERRE) Issue Paper. 09/2023.

Len, J., Ghosh, E., Grubbs, P., & Rösler, P. (2023). Interoperability in End-to-End Encrypted Messaging. Cryptology ePrint Archive, Paper 2023/386. Available at https://eprint.iacr.org/2023/386

Rescorla, E. (2022a). End-to-End Encryption and Messaging Interoperability. Educated Gueswork Blog Post. Available at: https://educatedguesswork.org/posts/messaging-e2e/#identity.

Rescorla, E. (2022b). Discovery Mechanisms for Messaging and Calling Interoperability. Educated Gueswork Blog Post. Available at: https://educatedguesswork.org/posts/messaging-discovery/

Rösler, P., & Schwenk, J. (2023). Interoperability between Messaging Services Secure Implementation of Encryption. Study for the German Federal Network Agency. Available at https://www.roeslpa.de/files/230503_dmaSecureReport.pdfhttps://www.roeslpa.de/files/230503_dmaSecureReport.pdf

Scott Morton, F. M., Crawford, G. S., Crémer, J., Dinielli, D., Fletcher, A., Heidhues, P., & Seim, K. (2021). Equitable Interoperability: the "Super Tool" of Digital Platform Governance. Policy Discussion Paper No. 4, Digital Regulation Project, Yale Tobin Center for Economic Policy. *Available at SSRN* 3923602.

Wiewiorra, L., Steffen, N., Thoste, P., Fourberg, N., Tas, S., Kroon, P., Busch, C., Krämer, J. (2022). Interoperability Regulations for Digital Services. WIK Consult Report. Study for the German Federal Network Agency. Available at

https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Onlinekomm/Study_InteroperabilityregulationsDigiServices.pdf?__blob=publicationFile&v=1

cerre Centre on Regulation in Europe

DATA-RELATED OBLIGATIONS IN THE DMA

ALEXANDRE DE STREEL
GIORGIO MONTI

1. INTRODUCTION

In this paper we discuss the four data-related obligations in the DMA. Each of the four rules is discussed using the following structure: (1) purpose and content of the rule, (2) principles for implementation and (3) relationship with other rules.

Identifying the purpose of these provisions and how that purpose is translated in the legal text matters because it allows us to see how far the rules are capable of supporting the objectives set and because EU law is interpreted having regard to the purpose of the rules. Our view is that **the data-related obligations predominantly pursue the aim of contestability. In this context, it is worth noting that in making markets more contestable attention is paid to dynamic competition**. A useful distinction in this respect is between sustaining and disruptive innovation. Sustaining innovation occurs when a firm creates a better performing service (e.g., a taxi company improves its online booking system), while disruptive innovation creates new markets (e.g. Uber). The DMA should support both.

The discussion then moves to how these rules may be complied with. Here we suggest that two legal principles matter: (i) effectiveness; (ii) proportionality:

- Every rule aspires to be **effective** but the DMA is particularly focused on ensuring that gatekeepers comply in a manner that achieves some change in the market – it follows that the Commission will look closely at the design of compliance and will ask for a reflexive approach by gatekeepers by which they revisit their compliance methods regularly. How this is achieved is the subject of the companion paper on DMA process and compliance. At the same time, effective compliance should not lead to gatekeepers implementing solutions that do not reflect consumer preferences.
- **Proportionality** means that the gatekeeper is expected to implement the obligations in a way that is effective but not disproportionate in achieving the objectives of the DMA. This balances the business freedom of the gatekeeper with the interests of opening up markets. More specifically, if there are two, equally effective ways of complying, then the gatekeeper may take the least onerous way.

There is a possible tension between proportionality and effectiveness because a regulator has a preference for the most effective method of compliance but the gatekeeper is not bound to maximise the effectiveness of the DMA, only to comply with the rules. The gatekeeper does not have a 'special responsibility' to make markets work better.[80]

In the third segment of each part, we discuss the relationship between the DMA obligation under discussion and other DMA rules as well as other rules of EU Law, especially the General Data Protection Regulation (GDPR).

[80] As is well-known the ECJ has held that a dominant undertaking has a special responsibility but even there it is a responsibility not to harm competition, not a responsibility to make markets more competitive.

2. ARTICLE 5(2) DMA

2.1. Purpose and Interpretation

2.1.1. Purpose

It is important to recall that Article 5(2) does **not prohibit the continuation of a business model based on data collection** by gatekeepers. While this model has been the subject of criticism, the DMA simply places limits on data collection by requiring explicit consent on the part of the user. The primary purpose of this limit is to make markets more contestable.[81] **Contestability is expected to manifest itself in three markets**.

First, limiting the data collection capacity of gatekeepers means that rival providers of core platform services have a more level playing field. Presently the concern is that the gatekeeper gains advantages by accumulating data and this raises entry barriers.[82] Contestability is enhanced in the market of those CPSs. This objective is pursued in particular by Article 5(2)(a). To illustrate, a new video-sharing platform service would be better able to compete with the gatekeeper video-sharing platform because the gatekeeper would no longer have the same data advantage as before to attract advertisements: each service would just acquire its own data. It may also improve contestability in the market of AdTech services to third parties as a new entrant in this market is unable to combine the same volume of data as incumbents. Of course, data only gives the gatekeeper one competitive advantage and there are multiple other factors that can affect entry but the DMA considers data accumulation to be a major entry barrier.

Second, Articles 5(2)(b), (c), and (d) seek to improve competition on the end-user side of the platform by facilitating the entry of new services provided by parties other than the gatekeeper. If users do not consent to data sharing, then the incumbent has a less pronounced data-related advantage and new entrants can compete by offering new services on a level playing field. Here contestability is supposed to be enhanced on the platform-to-consumer side of the market by limiting the capacity of a gatekeeper to leverage the data-related advantage it might otherwise have to enter new markets.

Third, **by limiting the capacity of data to be cross used for advertising, this makes the online advertising market more competitive**. This was the theory of harm in *Google/Fitbit* which was addressed by Google committing to create a data silo so that Fitbit's user-generated data would not be used to develop Google's online advertising market at the expense of others.[83] On the facts of that merger, the data could be used for other purposes but these uses will be governed by Arts 5(2)(b) and (c) in the near future.

However, the achievement of the purposes of Art 5(2) can be affected by the gatekeeper securing consent from users to collect personal data. If sufficient users' consent, then the existing market dynamics might not change. This is the most complex aspect of Article 5(2) DMA: **given that gatekeepers whose business model relies on data will probably seek to continue to secure consent**

[81] DMA, Recital 36 clarifies this.

[82] DMA, Recital 56.

[83] Commission Decision of 17 December 2020, Case M.9660 *Google/Fitbit*.

from users, how can this be achieved lawfully? And how far does the DMA constrain this business model? This is the main question discussed here before explaining in more detail what Article 5(2) forbids. Another wider question is whether the consent option risks frustrating this obligation altogether, but this is beyond the scope of this paper.

2.1.2. Content of the prohibition

Article 5(2) prohibits four actions relating to the collection of personal data from users unless there is explicit consent. Personal data means information about an identified or identifiable natural person (the data includes for example: name, location, physical attributes, mental state, economic circumstances, what a person likes and if a person visited a specific website).[84] This kind of data is valuable to advertisers who can offer better targeted ads to users and to platform service providers who can personalise their services or develop new products by understanding consumer demand better. Below we provide an interpretation of the various subsections of Article 5(2).

Art 5(2)(a) prohibits processing personal data of end users which they make available when using the services of third parties who make use of the gatekeeper's CPS if that processing is for the purposes of providing online advertising services.

- The personal data covered by this prohibition may be processed provided it is used for any other purpose. This is different from the other subsections of Art 5(2) which forbid data collection for any purpose. It does not include the use of his data for providing a gatekeeper's own advertisements but this use is regulated by Article 6(2).
- It is not clear what other purposes may be. Recital 36 speaks about developing custom audiences. This would seem to suggest that the data is used to help improve the service offered by the gatekeeper. However, note that the collection and processing of this data for these purposes still requires compliance with the GDPR.
- One should distinguish between (i) a situation where the end-user contract is with a third party but the gatekeeper offers the third-party service, which is covered by Art 5(2)(a) and (ii) a situation where the end-user's contract is with the gatekeeper who also supplies the service, which is covered by Article 5(2)(b) and (c).
- It may be argued that because this provision deals with data obtained when the end-user is using third party services hosted by the gatekeeper, that personal data which the gatekeeper obtains when the consumer uses services of the gatekeeper can be processed for the purposes of advertising. But this would be the wrong conclusion because this kind of data collection is regulated by the other provisions in Article 5(2).

Art 5(2)(b) prohibits combining personal data from the CPS under scrutiny with personal data from any other CPS (whether or not the firm is a gatekeeper in that sector), or any other services provided by the gatekeeper or with personal data from third-party services. This combination of data aims to harvest as much data as possible to identify new services, for example. The combination of data can

[84] GDPR, Article 4(1).

thus strengthen the gatekeeper's core platform service or other services. To a certain extent, even if users consent to combining personal data for the purposes of this provision, it is still the case that the principle of data minimisation in the GDPR applies, which places some limits on what gatekeepers may do with the data and how long they can store the data.[85]

- Unlike Art 5(2)(a), all combinations are forbidden, irrespective of purpose. In fact, this prohibition does not even explain whether or not this data combination is used by the gatekeeper in any way: what is forbidden is simply the combination of this data.
- Implicitly, the third-party services must be those services which use one of the firm's CPSs otherwise it is not clear how the gatekeeper can get hold of the data.
- The purpose of this prohibition seems to be that this data combination strengthens the gatekeeper's position in markets it is present in. For example, the data allows the gatekeeper to personalise a service to the user, or it can make search results more relevant. This benefits the consumer but the legislator is concerned that they also benefit the gatekeeper at the expense of rivals who would otherwise be able to enter the market.

Art 5(2)(c) prohibits the cross-use of personal data from the CPS under scrutiny in other services provided separately by the gatekeeper, including other CPSs.

- The differences with Art 5(2)(b) seem to be two: (1) here data is used, not just combined. However, the distinction between these two notions requires further clarification.[86] One interpretation is that the combination of data refers to a party putting together different data points and drawing inferences from them, while cross-use is about an active utilisation of the data in another market, as provided in the example below; (2) the other service is provided separately.
- The intention might be to address a leveraging scenario like the one addressed using Article 102 in the SEN/ENEL and the Engie cases where the incumbent energy provider used consumer data to enter a newly liberalised market: it had an advantage because it had the contact details of all eligible customers who could benefit from market opening.[87] Adapting this case-law to a digital service, it would mean a scenario where the gatekeeper uses the data to introduce a new service using the data to target this to those most likely to buy it.

[85] GDPR, Article 4(1)(c) :

[86] Centre for Information Policy Leadership, Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and
Practical Consequences Discussion Paper (May 2023) pp.13-14

[87] The Engie case was successful (Décision n° 17-D-06 du 21 mars 2017 relative à des pratiques mises en œuvre dans le secteur
de la fourniture de gaz naturel, d'électricité et de services énergétiques) but the SEN/ENEL case was not because the data was not commercially significant to give the dominant firm a competitive advantage (*Servizio Elettrico Nazionale v Autoritá Garante della concorrenza e del Mercato*, judgment of the Consiglio di Stato, 1 December 2022).

Art 5(2)(d) forbids the signing in of end-users to other services of the gatekeeper so as to combine personal data.

- This seems to describe one method of combining personal data which is dealt with by Art 5(2)(b).
- It follows that a gatekeeper can continue to provide a single sign-in for multiple services provided data is not combined. If someone does not consent to data combinations set out in Art 5(2)(b) then one may argue they should not be automatically signed in.

2.2. Implementation: How to Secure User Consent to Data Fusion

Article 5(2) allows the gatekeeper to process, combine, cross-use data or sign-in end users to other services to combine data if there is consent by the user. It is very likely that some gatekeepers whose business model relies on data collection will avail themselves of this exception and will try and secure user consent. Therefore, **the assessment of compliance is largely going to focus on whether consent has been obtained lawfully. It is for the gatekeeper to decide how to comply**. However, as we explain below, the DMA appears to indicate a preference for one way of complying. After explaining what that preference is, we show that it is not for the legislator to choose how the gatekeeper elects to comply.

2.2.1. The EU's preferred compliance path

Recitals 36 and 37 suggest one possible pathway to comply. This is just one possible option for gatekeepers, for otherwise the DMA would undermine the freedom of firms to run their business as they see fit as guaranteed by the Article 16 of the EU Charter of Fundamental Rights. The **compliance path found in the recitals** has the following components:

(i) The gatekeeper has to make available **two versions of the same service**.

a. One version is a 'less personalised but equivalent alternative' to the present service;

b. The second version may be described as the 'personalised' where the gatekeeper collects data which, absent consent, would infringe Art 5(2).

The less personalised version should be of the same quality as the version of the service that relies on data collection unless the degradation in quality is a direct consequence of the gatekeeper not being able to process the data. The assumption the legislator makes is that a gatekeeper today offers personalised version' only and so it is expected to roll out a less personalised version. The less personalised version may require the user to consent to handing over data so that the service may be offered in the first place, or the gatekeeper may be entitled to process data lawfully if this data is necessary to perform the contact. But no data that infringes the prohibitions in Art 5(2) may be collected for the operation of this less personalised version.

(ii) Users choose whether to sign up to the less personalised version or the personalised version.

(iii) The gatekeeper may allow the user to **opt in to a more personalised service** by giving consent to data processing. Consent must be sought proactively by providing a user-friendly interface for the consumer to decide whether to consent. Here compliance with GDPR principles of consent is necessary.[88] Nevertheless the DMA provides some further specifications which impose obligations that may be in addition to those under GDPR:

a. At the time of giving consent the user is advised that even if they do not give consent, the core platform service remains unchanged and no functionalities will be suppressed.[89] In other words, if you do not opt into the personalised version, you can still have the less personalised version;

b. Online interfaces shall not deceive, manipulate or materially distort the ability of the user to give consent;[90]

c. When consent has been refused, a repeat request for consent cannot be made more than once a year.[91]

This is not necessarily the only way to comply. First, Recitals are not legally binding. Second, as mentioned above it undermines the freedom to conduct one's business too far as there may be less onerous ways of complying. Third, it feels commercially unrealistic for some: it assumes that on the day when compliance starts, every user is automatically 'demoted' to a less personalised service and is then asked to consent to a system upgrade by giving over more data. Can this really be what is intended? **Less onerous alternatives can be explored and some are sketched below. However, it is worth noting that Meta's discussions with the Bundeskartellamt (BKA) as well as the judgment of the ECJ in *Meta v BKA* seem to go in this direction**.[92] Both are considered here briefly.

Meta's new accounts centre: users are given the option to combine their various Meta accounts so that Meta could combine the data. The BKA focused on whether the steps were transparent and comprehensible for the user, whether the process to separate the accounts was sufficiently simple. **Meta is allowed to make it clear that by consenting to hand over data by combining accounts that the user gains additional functionalities, for example cross posting the same user-generated content on two social media platforms. The BKA makes it clear that a remedy of this nature addresses the competition concerns it identified** but that this is not necessarily a solution that complies with the DMA or new provisions found in German competition law. However, with regards to DMA compliance, it seems clear that the remedy is in line with the compliance pathway envisaged by the DMA.[93]

[88] The DMA refers specifically to art 4(11) and 7 of GDPR. The elements of consent are discussed elsewhere, see for example EDPB, Guidelines 05/2020 on consent under Regulation 1016/679 (May 2020). See also C-61/19

[89] See for this DMA, Recital 37 and Art 13(6)

[90] DMA, Recital 37 and Art 13(6)

[91] Art 5(2).

[92] Case C-252/21 Meta Platforms v Bundeskartellambt, EU:C:2023:537.

[93] https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/07_06_Meta_Daten.html

Meta v BKA: here the question arose whether Meta's dominant position in the market for online social networks had any role to play in determining the question of consent. While the Court of Justice rightly held that dominance does not preclude the possibility of giving consent, **market power was relevant to assess if content was freely given**.[94] The Court linked this factor with Article 7(4) GDPR:

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

With reference to the facts of the case, the ECJ thought that the processing by Meta was not 'strictly necessary' for the performance of the contract between Meta and users.[95] It follows that users should be free 'to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.'[96] Here too the hint (it can only be a hint because the ECJ cannot answer questions of fact in a preliminary ruling) is that a **dominant firm wishing to secure user consent to data must offer an alternative way of accessing the service to one that requires the consent to handing over data**.

However, there must be other ways for gatekeepers to comply with Article 5(2) and some options are discussed below.

2.2.2. What less onerous alternatives might be considered?

A first option would be that, on the date when compliance is due (i.e. six months after the gatekeeper designation), **the gatekeeper gives users a take it or leave it offer**: you may use this service if you continue to consent to data collection or you are no longer entitled to the service. After all, neither the DMA nor any general principle of EU law compels a firm to do business with any user unless there is a specific obligation imposed by law.

To a certain extent, the judgment in *Meta* seems to run counter to this intuition because it assumes that for the purposes of ensuring that the user consents freely (based on a joint reading of Article 102 and the GDPR), she must have a choice between two viable options to contract with the gatekeeper: by handing over data or by not handing over data. This is a striking interference into freedom to run one's business: it seems that dominant firms cannot provide a product that relies on extensive data extraction if the user cannot obtain that product without handing over data. This results from a joint reading of Art 102 and GDPR and is not an innovation brought about by the DMA, which does not impose a requirement to offer a less personalised and a personalised version for the user to select. However, it is arguable that since the DMA makes reference to the GDPR and that most likely a gatekeeper enjoys market power akin to dominance, that the holding in Meta can be transposed to

[94] Meta (above n 13), para 148

[95] Meta (above n 13), para 149.

[96] Meta (above n 13), para 150.

the DMA. If so, then a take it or leave it option is not feasible. It might even be challenged as contrary to the spirit of the DMA which is to facilitate user choice rather than prevent it.

A second option could be for the **gatekeeper to offer a paid-for service where data is not processed** in ways contrary to Article 5(2) and a free service in exchange for data. A question arises if the price of the paid-for service is too high whether this would be read, following the *Meta* judgment, as de facto not a choice at all, and so contrary to Art 102 TFEU.[97] However, it may be consistent with the DMA.

A third option could be for the **gatekeeper to buy user data**. After all, the economic value of the gatekeeper is in part sustained by its users clicking and staying on the platform as long as the platform can retain their attention. Nothing prevents this under the DMA: consent is obtained when the user agrees to be remunerated for agreeing to have their data used, but it is not likely that a gatekeeper would consider this option.

A fourth option, the rationale for which will become apparent in section 2.2.3 below, is **that the gatekeeper provides one less personalised service and then a range of more personalised services**, each of which requires that the user consents to some data being used. For example, a slightly more personalised service if the user consents to allow the data to be combined with other data, a more personalised one if the user consents to the data being used for advertising purposes and so on.

In sum, as a matter of law, the DMA cannot compel a firm to design its business in a specific way. It can only forbid certain business models when these are inherently contrary to the DMA provisions. Within that parameter, a gatekeeper has a certain leeway in choosing how to comply. Some options were canvassed here as a way of illustrating the various options available. The common denominator is that whatever option is adopted, the user must consent and this leads us to discuss how gatekeepers should be expected to make choice possible.

2.2.3. How to design the end-user's choice?

One difficulty in implementing any of the approaches sketched above is that **the gatekeeper has to inform the user of multiple data collection practices where that arises**. The user should opt in to each one. An end-user for example may be willing to consent to data being processed for advertising purposes (Art 5(2)(a)) but may want to deny giving consent for the other two purposes in Art 5(2)(b) and (c). So, then a **gatekeeper has to offer a menu of consent options when providing the so-called 'personalised service'. Alternatively, the gatekeeper can present individual choices at different times and not all at once.** This would seem to be the requirement under the GDPR.

Here there is a tension. Consider a gatekeeper who offers two options: a less personalised option and a personalised one, where all data collected for all purposes in Art 5(2). This might not satisfy the DMA requirements because the user's choice is not sufficiently specific, and this may not be sufficient for the purposes of the GDPR either. However, the user might understand this choice relatively easily and decide if they are happy for data to be used.

[97] For discussion see F. Scott Morton, 'Meta's Offer' VoxEU Column 13 December 2023.

Consider instead a gatekeeper that offers a less personalised version and a personalised option where the user decides which data uses it consents to, one tick box for every provision in Art 5(2)(a), (b), (c) and (d). This allows the consumer to give specific consent, but will a user read this, and if they do will they understand the implications of each choice?

In sum, the point we suggest here is that offering just two options, a less personalised one without data collection and a personalised one with all data collected, may be a choice a user understands well and can make a decision in an informed manner. Conversely, a choice that asks the user to give specific consent to each and every use of data may be one that users do not understand as clearly and may not make choices that represent their preferences. In sum, the DMA might be more effective if two options are presented, but the gatekeeper is more likely to be compliant if it offers a less useful choice menu with multiple choices. While this interpretation runs counter to the idea of consent embedded in the GDPR and the DMA, some realism is needed on the part of the enforcers: we cannot regulate on the assumption that users have high levels of literacy and read every word attentively when asked to consent.

This is where a trade-off is needed: a solution which on paper maximises user choices but it is overly complicated for users to understand means that many users risk making choices that do not correspond with their preferences. Conversely, a more modest set of choices may not be perfect but the user would be able to understand what they are choosing. Effectiveness as a general principle might indicate that the latter is a preferable solution.

There may be a long-term solution, drawing on how user choice has been simplified in other fields. For example, since we know that consumers do not read or understand how unhealthy certain foods are a **simple labelling system** is used to indicate calories in food (red, yellow, green). For white goods energy consumption standards are simplified with energy labels because few consumers would understand the numbers provided by manufacturers. Might a similar approach be used for gathering data consents for the purposes of Article 5(2)? It is beyond the scope of this paper to discuss this fully but briefly one might imagine a scenario where a gatekeeper labels its choice options along a scale the colours serving as a proxy for the amount of data you hand over (green no data collected, red all data collected), or industry participants can agree on setting standards for data use, or the EU can legislate to set these.

The literature assessing labels for food content and energy consumption gives mixed results: policymakers seem to agree that this can be a helpful measure but the evidence suggests that the design of these simple information tools is difficult and that they may affect certain classes of consumer above others. For example, one study reveals that the EU energy label does not increase demand for energy-efficient goods while information about the lifetime costs of operating the goods

increases demand for energy efficient products.[98] However another study finds the opposite.[99] These differences are explained by a third study which concludes that 'the specific national context in which an intervention is implemented is a key determinant of its effectiveness.'[100] Another reviewing several studies points out that nutrition labels have little effectiveness among people in a low socio-economic position.[101] The takeaway is that **effective design is a challenge but it seems to provide better results than not providing consumers with the capacity to make choices based on simple heuristics**.[102]

2.2.4. The contents of a less personalised version

Another difficulty that arises should a gatekeeper decide to roll out a less personalised service is working out what a lawful less personalised service consists of. Given that many gatekeepers have been offering services with extensive data collection, **how can one determine if the less personalised service is of an appropriate quality** or if the gatekeeper has degraded the conditions or quality of the CPS provided to users who avail themselves of the rights in Article 5(2)?

Consider for example cross-posting, the practice of making it possible for a user to post the same content simultaneously on two platforms owned by the gatekeeper. Suppose that in pre-DMA times all users had the ability cross-post but data was collected and combined. The gatekeeper now designs a less personalised version of the service without data collection: must this basic version allow for cross-posting or can cross-posting be only made available if the user consents to some data sharing? Further discussion of this question probably requires us to know more about how a platform works, but a reasonable assumption is this: in order to make cross-posting happen, the platform necessarily has to have and use some personal data from the user so that it can match the user's two accounts. It is likely that the gatekeeper must, using the terms in Art 5(2)(c), cross-use some personal data. So, in this way, **cross-posting is definitely not a part of the less personalised service** because that service must be available without collecting some data forbidden by Art 5(2) DMA and the gatekeeper must ask for user consent.

One more key observation may be made drawing on the example above: assume that the gatekeeper proves that it cannot offer cross-posting under the less personalised service because it can only offer it by cross-using personal data. This does not mean that the gatekeeper, when offering the user the option to opt in to the personalised service which includes cross-posting, is limited to seeking consent for those uses forbidden by Art 5(2) which are necessary to offer the service. The gatekeeper is free to offer the more personalised service on condition that the user gives consent to all data collection

[98] M.A. Andor, A. Gerster, L. Götte, 'How Effective is the European Union Energy Label? Evidence from a Real-Stakes Experiment' (2019) Environmental Research Letters 14 044001.

[99] M. Skourtos et al 'Efficient Energy Labelling : The impact of Information Content and Style on Product Choice ' (2021) 14 Energy Efficiency, Article number 58.

[100] S. Ceolotto & E. Denny, 2021. 'Putting a new 'spin' on energy labels: measuring the impact of reframing energy efficiency on tumble dryer choices in a multi-country experiment' Trinity Economics Papers tep1521, Trinity College Dublin, Department of Economic

[101] D. Sarik et al 'The Impact of Menue Energy Labelling Across Socioeconomic Groups : A Systematic Review (2016) 99(1) Appetite 59.

[102] See generally M.A. Andor et al, 'Consumer Inattention, Heuristic Thinking and the Role of Energy Labels' (2020) 14(1) The Energy Journal 83.

prohibited by Art 5(2), subject to the discussion above regarding the need for consent to be specific and subject to compliance with GDPR principles.

These interpretations of Art 5(2) are summarised in a more general manner in the table below.

Determination of less personalised service	The gatekeeper can defend the provision of a less personalised service that lacks features available on the premium version by showing that the feature in question can only be offered if the user consents to the collection of some data otherwise forbidden by Article 5(2).
Scope of consent for the **personalised service**	The gatekeeper is free to require that the user consents to all data processing otherwise forbidden by Art 5(2) and is not limited to asking for consent for data processing necessary to deliver the personalised service.

The justification for these two interpretations (which might at first blush seem contradictory) should be clear. The less personalised service is defined by the DMA itself as a service that does not rely on data uses forbidden by Art 5(2). However, the burden of proof is on the gatekeeper to show that it cannot offer the service in question without using personal data listed in Art 5(2). This is where the compliance report can provide valuable information: it allows the gatekeeper to reveal how the platform works and what data is necessary to ensure that a service functions.

When it comes to the scope of consent, Article 5(2) does not limit the type of data use that the gatekeeper can ask consent for or make that depend on what additional services can be provided with that data. However, it is arguable that the DMA requires that the gatekeeper explains to users the services that can be provided to them or the benefits they might receive indirectly if they consent to the collection and use of data.

2.2.5. Data fusion under Arts 6(1)(c),(d) and (e) GDPR

The DMA provides that a gatekeeper can also combine data on three other legal bases and the judgment in *Meta v BKA* helps interpret each. These alternative legal bases are unlikely to be relied on frequently.

*Article 6(1)(c): processing is necessary for **compliance with a legal obligation** to which the controller is subject.*

Meta seems to have argued that it had a legal obligation 'to collect and store personal data in a preventive manner in order to be able to respond to any request from a national authority seeking to obtain certain data relating to its users.'[103] This would be something for the national court to consider.

In addition, the Court states that this is a legitimate legal basis only '(1) where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, (2) where that legal basis meets an objective of public interest and (3) is proportionate to the legitimate aim pursued and (4) where that processing is carried out only in so far as is strictly necessary.'[104]

*Article 6(1)(d): processing is necessary in order to **protect the vital interests** of the data subject or of another natural person*

The Court in Meta draws on Recital 46 GDPR to suggest that this provision deals with the protection of the life of the data subject or another natural person. Here 'in view of the nature of the services provided by the operator of an online social network, such an operator, whose activity is essentially economic and commercial in nature, cannot rely on the protection of an interest which is essential for the life of its users or of another person in order to justify, absolutely and in a purely abstract and preventive manner, the lawfulness of data processing such as that at issue in the main proceedings.'[105]

*Article 6(1)(e): processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.*

The question in Meta was whether it was 'entrusted with a task carried out in the public interest or in the exercise of official authority, in particular with a view of carrying out research for the social good and to promote safety, integrity and security.'[106] While this was for the national court to find out, the ECJ considered it was unlikely to apply.

In addition to providing guidance on the possible meanings of these three provisions, the Court insists that because data processing on **these legal bases is non-consensual that they must be interpreted restrictively**.[107] The burden rests on the gatekeeper to demonstrate that data combination or cross-use are necessary to achieve these goals. However, some have suggested that these legal bases are too narrow to protect users adequately.[108]

However, the **gatekeeper who wishes to take advantage of these alternatives cannot collect data for all the four uses forbidden by Art 5(2)**. In other words, based on the principle of proportionality the gatekeeper has a duty to show which data it must collect or use in order to discharge the

[103] Meta (above n 13), para 132.
[104] Meta (above n 13), para 138 (numbers added for clarity).
[105] Meta (above n 13), para 137.
[106] Meta (above n 13), para 133.
[107] Meta (above n 13) para 93.
[108] See some examples and discussion by Centre for Information Policy Leadership (above n 7) pp.16-19.

obligations in Articles 6(1)(c), (d) or (e). For example, if the gatekeeper states that processing 'is necessary for compliance with a legal obligation to which the controller is subject' then it has to explain which of the forms of processing forbidden in Article 5(2) it must be allowed to carry out. It seems difficult to imagine a scenario where the legal obligation would require that the gatekeeper processes data for the purposes of providing online advertising forbidden by Art 5(2)(a) but it may be that combining personal data of user from multiple platform services is necessary if there is legislation requiring, for example, that a social media provider collects all data about user online activity. However even here this collection of data on user activity cannot be used to secure a competitive advantage. Thus, these three additional legal bases allow the collection of data for reasons that are not going to affect fairness or contestability.

2.3. Relationship with Other EU Legal Provisions

2.3.1. Between Art 5(2) and Art 15 DMA on auditing profiling techniques

Article 15 requires that gatekeepers perform an audit of techniques for profiling consumers that are applied in the CPS. This is transmitted to the European Data Protection Board and the gatekeeper must also provide a publicly available overview. It is not clear how this reporting obligation helps the enforcement of the DMA. However, the intention behind the public report is to facilitate contestability: by making it more transparent for users how the gatekeeper collects and uses their data, this can make it possible for 'other undertakings providing core platform services to differentiate themselves better through the use of superior privacy guarantees.'[109] It can be doubted that these reports are valuable for end-users to gain a better understanding of what their data is used for and thereby strengthen their capacity to consent. Some consumer organisations may use these to facilitate user understanding though.

However, the DMA does not require a shift to a data collection-free market for any core platform service. Rather, it creates the possibility for competition to emerge based on privacy settings. It does not stop a new entrant from competing against a CPS by itself gathering as much data as is lawfully possible. The legislation is agnostic about which business models might emerge once markets become more contestable. This matters: laws can encourage the development of preferred market outcomes but very rarely do laws ban certain markets out of existence.

2.3.2. Relationship with other EU rules

Article 5(2) creates a system whereby when the gatekeeper secures consent, it does so in a manner that is GDPR compliant. As discussed above it seems that **in order to collect data covered by Article 5(2) by securing user consent, the DMA imposes further procedural requirements**: the gatekeeper cannot ask for consent repeatedly; the gatekeeper cannot use dark patterns to secure consent; refusal to consent cannot deprive the user of a service without data collection.[110]

[109] DMA Recital 72.

[110] See also ICO, CMA and DRCF, Harmful Design in Digital Markets : How Online Choice Architecture practices can undermine consumer choice and control over personal information (9 August 2023). https://www.drcf.org.uk/__data/assets/pdf_file/0024/266226/Harmful-Design-in-Digital-Markets-ICO-CMA-joint-position-paper.pdf. See also Amelia Fletcher's paper in this series.

It is worth stressing that the **DMA is not some sort of GDPR+ regime** such that the fundamental rights of data subject are protected better because of the DMA. The purpose of the DMA is not to enhance the rights of data subject. This objective may nevertheless be achieved indirectly because the DMA adds the procedures summarised above to gatekeepers and because it stimulates the emergence of business models that rely less on personal data.

3. ARTICLE 6(2) DMA

3.1. Purpose and Interpretation

3.1.1. Purpose

This provision is based mainly on the contestability aim of the DMA. It may also be explained as being about fairness because otherwise the gatekeeper takes advantage of data which has been generated thanks to business users. It is designed principally to level the playing field in markets where the CPS offers a distribution service for business users to reach consumers. Gatekeepers who use the data of the business users that are present on its platform are able to leverage into the market occupied by those business users, and Art 6(2) prevents this. Thus, the market where this obligation **creates contestability is the market for goods or services provided to end users through the CPS**. This is perhaps surprising because this could be any market, not necessarily a digital one.

Whether Art 6(2) **may also make any of the CPS markets more contestable is less certain** although it is possible that a disruptive innovator begins by relying on the CPS to gain scale and then becomes itself a CPS. For example, a firm making widgets might start selling these on Amazon, but it may then gain sufficient numbers of customers that its website becomes the go to place for buying widgets and other widget producers ask to sell their goods on that platform in preference to Amazon. Amazon, unable to use that business user's data, cannot compete against it in the widget market as easily as it could before this obligation came into force. However, it is not clear that Article 6(2) on its own can contain a gatekeeper to such an extent that a rival can enter the CPS market.

3.1.2. Interpreting the obligation

*What is the obligation about**?***

Users of gatekeeper services generate data while using the CPS. Some of this data is personal data generated by customers of the business users. This data becomes accessible by the CPS in order to facilitate the transaction between the business user and the consumer. Data may be discrete: about a specific transaction (Joe Bloggs bought a Barbie doll on 1 June 2023) or aggregated (based on the transactions on the platform, consumers in the UK aged between 40 and 50 buy a lot of Barbie merchandise and pink goods). This data can be useful for the business user because they can gauge demand and develop new products. In the hands of a gatekeeper, this data allows it to leverage its position into those markets where there is demand. Obviously if the same data is also available publicly, then the gatekeeper is free to use that public record.

To which CPS does this provision apply?

Some are clearly within the scope: app stores, marketplaces, virtual assistants. Less clear if this also applies to search, advertising or social networks. The test is whether there are business users that rely on the CPS to offer goods or services downstream.

Recital 46, final sentence reads: 'That obligation should apply *to the gatekeeper as a whole*, including but not limited to its business unit that competes with the business users of a core platform service.' This means that the **obligation applies to all the gatekeeper's entire line of business, all the core**

platform services that it operates but also, it seems, any other lines of business. This is necessary because if the idea is to prevent leveraging data, then this risk is mitigated only if that data may not be used for the purposes of competing with the business user. It means the obligation applies to the enterprise as a whole, beyond the technology segments identified by the DMA.

What data?

The text is drafted to encompass a wide range of sources of data by including both data generated by the business user or by the consumer using the services of that business user. It does not seem that the data need necessarily lead to a transaction being concluded between the business user and the consumer, thus search data is within the scope.

Data which is subject to this obligation must be '**not publicly available**.' The burden of proof should be on the gatekeeper to reveal that the data is available elsewhere and not on the business user to show this. After all the presumption should be that the data about how frequently consumers search or buy a particular good is not available to the public.

Finally, on the concept of data, consider these questions:

1. The data cannot be used 'in competition with business users.' This raises a question about whether these are actual or also potential competitors. For example, the business user sells a mousetrap through the CPS and the gatekeeper uses that data to develop a trap for cockroaches using that data. Is this illegal use of the data?

2. Is old data outside the scope? Can a gatekeeper say that data gathered 5 years ago can no longer serve to give it a competitive advantage?

3. what about data from past business users?

These questions raise an issue about how to interpret the DMA. A **literal reading would allow to give a fairly broad interpretation** in some cases (all business users, past and present and even old data), and if this is over-inclusive this is irrelevant because the purpose of the DMA is to make application as clear as possible, Type 1 errors are accepted. Conversely, a **purposive reading would allow to narrow down the scope** of the data to be 'siloed' by claiming that some data is not valuable for the purposes of leveraging.

But to make matters trickier, a purposive reading could also help widen the scope of data for example by extending it to potential competition because the aim is to make markets contestable and allowing the gatekeeper to use data to develop new products enhances the gatekeeper's power at the expense of rivals. This may be supported by the importance to stimulate dynamic competition which is served by offering business users a wide range of data so that they may discover new products.

One caveat may be entered: if the gatekeeper makes the data publicly available, then the data is no longer subject to this obligation. Might it be to a gatekeeper's interest to make such data publicly available so that it too may use it? For example, aggregated data which does not identify users and

therefore is not subject to GDPR protections could be published and then it could be used by both business users and end users.

Which business users benefit from Art 6(2)?

The answer is on the whole fairly clear: **those who use the CPS, but some borderline cases** are worth exploring: (i) business users who have been terminated by the gatekeeper for legitimate reasons (e.g. a business user who does not comply with the gatekeeper's terms and conditions); (ii) business users who have stopped using the CPS, because they have opted to use another CPS to offer their goods/services? How to decide if these are to be included?

3.2. Implementing the Obligation

The shorthand for Art 6(2) is that this is a provision about creating 'data siloes'. This description is a little too simplistic because the silo is composed of data for a specific purpose. Data generated by a business may be used legitimately by the gatekeeper (e.g. to improve a search function on the platform). These legitimate uses are pro-competitive because the gatekeeper uses data to rank results in a manner that is favoured by consumers. However, recall that if the gatekeeper processes personal data in order to achieve this, it must have a lawful basis under the GDPR.

It follows that it is important to be clear that it is **only *specific uses of the data* which are forbidden and placed in a silo**. It follows that this is not a rule that prohibits the gathering of such data. This has implications for the enforcement of this obligation.

The only way to verify compliance would be to offer access to the data management plans of the firm so that the use of the relevant data can be audited: who is given access to it, in which workflows does the data go? Are there clear and fail-safe protocols to ensure that the data does not flow to that business unit which might use the data to develop goods/services that compete with those of business users?

A useful model for what is expected may be the data remedy in *Google/Fitbit*.[111] Space prevents a full account, but these are the key points from that decision that also apply to DMA compliance which reveal that these commitments hold some information about how the Commission may wish to see the DMA implemented:

The identification of the data and the definition of the scope of uses that is out of bounds as well as which Google workers who may access the data for other legitimate purposes.[112] The decision reveals that this needs to be specified carefully. For example, the commitment includes 'the obligation to compile specific and detailed access documentation in relation to individuals and services that will have access to the relevant data, in order to facilitate the monitoring of Google's compliance with the related obligations. Minimum data and information points subject to periodic audits are also introduced. The improvements appear able to limit the risk of circumvention and of misuse of the

[111] Commission Decision of 17 December 2020, Case M.9660 *Google/Fitbit*.

[112] The Commission speaks of a 'strictly permissioned data storage environment' that holds the data and of 'strictly permissioned temporary logs' which hold the data for specific and permitted processing facilities. Ibid., para 862.

relevant data and in case give the Monitoring Trustee an increased ability to deter violations and to address them.'[113]

Having a Monitoring Trustee who is technically capable of checking that there is compliance and that they have access to 'the technical means through which data separation is granted.'[114]

Moreover, the Monitoring Trustee should be able to assess 'the adequacy of the technical means through which data separation is obtained.' [115]

In turn, it follows that the Monitoring Trustee must have adequate technical abilities and expertise.

Specifying that Google may change the technical means to comply with the data separation commitment as new technologies and standards evolve, with the proviso that changes are supervised by the Monitoring Trustee.[116]

It seems that for the purposes of the DMA the monitoring function is for the compliance function unit. Furthermore, from a procedural perspective, it seems that this remedy is probably best designed with stakeholder input and with a steer from the Commission.

3.3. Relationship with Other EU Legal Provisions

3.3.1. Between Art 6(2) and Art 5(2)

These two data-related obligations work **independently of each other**. The simple fact that the gatekeeper has obtained the consent of the user under Article 5(2) does not allow the gatekeeper to use that personal data for the purposes listed in Art 6(2).

To make this more concrete: The user logging on to a CPS transmits personal data directly to the gatekeeper. The gatekeeper might well obtain consent under Article 5(2). However, this cannot allow the gatekeeper to use this data for the purposes of Article 6(2). The prohibition in Article 6(2) is *per se*: no user consent can override it. Any other reading would make Article 6(2) easy to circumvent.

3.3.2. Between Art 6(2) and 6(10)

Article 6(2) **forbids the gatekeeper** from accessing certain data. Article 6(10) requires the gatekeeper to **provide data to** business users.

Article 6(10) includes the same data as Art 6(2) (i.e. that which is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services) but it also includes personal data generated or provided by 'end users engaging with the products or services provided by those business users.'

[113] Ibid., Para 966(e). See also para 897 for a detailed list of points to be defined.
[114] Ibid., Para 959
[115] Ibid., Para 967(b)
[116] Ibid., Para 863

3.3.3. Relationship with other EU rules

Perhaps for completeness Art 6(2) includes personal data, but any GDPR compliance measure is irrelevant for the purposes of interpreting this obligation, except for the question whether the gatekeeper can use that personal data for purposes other than competing with business users, in which case that use would have to be lawful under this provision but falls to be regulated by Art 5(2) and the GDPR.

However, it must be made clear that **Article 6(2) has nothing to do with the GDPR duties**: the data subject has no rights under Article 6(2) of the DMA. However, the gatekeeper might have some GDPR duties nonetheless. For example, if the consumer buys a good form a gatekeeper platform which is sold by a business user of the gatekeeper then some data about the consumer has to be transferred from the business user to the gatekeeper to complete the contract. There are GDPR obligations in this relationship but these operate independently of the DMA. The gatekeeper platform may be a joint controller and have to demonstrate a legal basis for processing the information.

Finally, the notion of 'use' under this provision of the DMA is not based on this use being lawful or unlawful under GDPR: use is illegal when the data is processed to gain an economic advantage over a rival.

4. DATA PORTABILITY AND ACCESS FOR END USERS AND BUSINESS USERS: ARTICLE 6(9) AND 6(10)

4.1. Purpose and Interpretation

Next to the prohibitions, the DMA imposes also obligations related to data access and sharing. This paper focuses on the two data portability and access obligations benefiting end-users (Art.6.9) and business users (Art.6.10). [117]

First, Article 6(9) augments the data portability right of the GDPR and provides that:

The gatekeeper shall provide **end users and third parties authorised by an end user**, at their request and **free of charge**, with effective portability of **data provided by the end user or generated** through the activity of the end user in the context of the use of the relevant core platform service, including by providing, free of charge, **tools** to facilitate the effective exercise of such data portability, and including by the provision of **continuous and real-time** access to such data. (our underlining)

Recital 59 clarifies the objective of the obligation which is related to the general objective of the DMA (i.e., market contestability and distributional fairness) in the following way:

> *(…) to ensure that gatekeepers do not undermine the **contestability** of core platform services, or the innovation potential of the dynamic digital sector, by **restricting switching or multi-homing** (… which) should lead, in turn, to an increased choice for end users and acts as an incentive for gatekeepers and business users to innovate.* (our underlining)

Second, Article 6(10) creates a new data portability right for business users and provides that:

The gatekeeper shall provide **business users and third parties authorised** by a business user, at their request, **free of charge**, with effective, **high-quality, continuous and real-time access** to, and use of, aggregated and non-aggregated data, including personal data, that is **provided foror generated** in the context of the **use of the relevant core platform services or services provided together** with, or in support of, the relevant core platform services by those businessusers and the end users engaging with the products or services provided by those business users.

With regard to **personal data**, the gatekeeper shall provide for such access to, and use of, personal data **only where the data are directly connected with the use** effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users **opt in** to such sharing by giving their consent. (our underlining)

The objective of this second portability obligation is not explicitly clarified in the DMA, but the obligation contributes to (i) contestability as it facilitates business users switching and multi-homing, (ii) innovation as it stimulates data-driven innovation by business users and (iii) fairness as business users would be more control of 'their data'.

[117] This part draws on J. Kramer, Data Access provisions in the DMA, CERRE Report, January 2023.

Thus, the "data mobility" stimulated by the new DMA data obligations would increase contestability, fairness and ultimately innovation on the EU digital markets. However, it is absolutely key that this new data mobility does not undermine data privacy and security and ultimately the trust of the users in the (big and small) providers of digital services and, more generally, in the digital society. For this, privacy and security risks should be managed carefully by all stakeholders involved in the increased data mobility framework and users should be educated to the possibilities and risks of these new choices.

4.2. Implementing the Obligations[118]

The data portability and access obligations create optional choices for end and business users, and therefore it would be important that the **choice architecture follow the legal and economic principles specifically mentioned in the companion paper on choice architecture i.e. effectiveness, proportionality, non-discrimination as well as the 'Attend, Access, Assess Act' choice framework, ex ante testing and ex post assessment**.

Besides those principles applicable to choice architecture, the implementation of the data related obligations should also respect three general good regulatory principles: effectiveness and proportionality, participation and non-discrimination.

4.2.1. Effectiveness and proportionality

The implementation of the data related obligations should be based on two main general EU principles:

The principle of *effectiveness* is a general principle of EU law and is also mentioned generally in the DMA (Art.8.1 with sets out a double effectiveness principle, with regard to the data portability obligation and with regard to the DMA twin objectives) and specifically mentioned for each data portability obligation;

The principle of *proportionality* which is also a general principle of EU law

To ensure effectiveness, the data portability and access should be properly managed. The data transfer needs to be secure, minimising risks for data leakage to parties not involved in the transfer, data modification or loss of data.

In particular, it is key that the authorised third party receiving the user's data under Article 6(9) can be trusted and must adhere to the GDPR and adequately protect the data in their respective systems, not only during the transfer, but after the transfer takes place. Furthermore, authorised third parties should be expected to use the data for the purposes underpinning 6(9), which are for switching and multihoming and should not sell/further transfer/use the data for other purposes without expressly informing users prior to any transfer. Without implementing independent harmonised privacy and

[118] J. Krämer, P. Senellart and A. de Streel, Making data portability more effective for the digital economy, CERRE Policy Report, June 2020 and R. Feasey and A. de Streel, Data sharing for digital markets contestability, Towards a governance framework, CERRE Report, September 2020

security standards/verifications that third-parties ought to meet before they entice users to port their data and begin pulling their data from gatekeepers, the risks to data security of EU citizens increase.

Moreover, experience of the implementation of previous portability obligations, such as number portability between telecommunications operators or data portability between financial institutions within the context of Open Banking[119] suggests that there are **opportunities for the data holders to hinder the transfer**. Thus, a prerequisite for the effective implementation of new data portability obligations will be trust on the part of the business and end users who stand to benefit from it. Unjustified actions that create unreasonable doubt or uncertainty about the reliability of the process, or the risks involved, will tend to favour the gatekeeper and reduce the volume of transfers that occur.

As explained in Kramer et al (2020), there are **various data models and formats** commonly used in the digital economy: 'These formats can be roughly categorised as structured, semi-structured and unstructured data. In both the structured and semi-structured cases, file formats only specify a syntactic layer on how information is represented. To make sense of it, it is necessary to know the schema of the data, i.e. what fields and data attributes exist, and what constraints on the data values should be respected. Beyond the syntax (provided by the file format), the schema and the constraints (given by the schema annotations, when available), data needs to be interpreted with respect to a specific semantics, which gives meaning to data fields and attributes. When data is exchanged between two data controllers using different schemas, it is necessary to transform it from one schema to the other, using schema mappings from the source to the destination. These schema mappings are, most of the time, hand written by data engineers, although there is sometimes the possibility of automated learning from examples.'

In that regard, the DMA provides that the gatekeeper will have to set up technical tools for an effective portability of data in continuously and real-time manner combined with the protection of privacy, security, and service integrity.

Recital 60 clarifies that the appropriate technical measures could:

> *consist of high-quality application programming interfaces or integrated tools for small volume business users.*

As mentioned by Kramer (2023), it will be important to **harmonise data formats and interfaces for data portability across the different gatekeepers** so as to allow third- party tools, such as Personal Information Management Systems (PIMS), to better integrate with the largest possible set of firms and thereby to facilitate switching and multihoming. In other words, instead of having one tool per gatekeeper, it would be better to have one tool that is able to connect to all gatekeepers for the purposes of data portability.

[119] Fingelton/Open Data Institute note that under the Second Payment Systems Directive, users are required to fully re-authorise their permissions every 90 days. Although ostensibly to reaffirm customer consents and retain customer control, this provides an incumbent platform with a periodic win back opportunity: 'The current PSD2 legislation requires a full reauthorisation every 90 days, which can make Open Banking products cumbersome for users and lead to user attrition for TPPs, increasing costs for them'. They suggest a cost benefit review is undertaken to assess the merits of this obligation.

When personal data are involved, an additional difficulty is the establishment of a **consent management** system which is effective and respect the GDPR requirements of Art.7 GDPR. Indeed, Recital 60 clarifies also clarifies that:

a gatekeeper should enable business users to obtain consent of their end users for such data access and retrieval, where such consent is required.

This relates to the **granularity** of consent, but may also include the possibility to give **automated consent**, for instance, through tools such as Personal Information Management Systems.

The consent management system will also require an effective **process of for user authentication.** As noted by Feasey and de Streel (2020), large digital platforms already offer their authentication services to third-party platforms which allow their users to connect to those platforms without the need to re-authenticate. Hence, the adoption of fingerprint, eye or facial recognition as a means of authenticating consents for data transfers might be leveraged if these firms are involved in the process. Regulatory oversight may be required to ensure that it is implemented in a manner which both safeguards the interests of users and achieves the objective of promoting competition.

4.2.2. Participation

The **process and technical tools could be determined by the gatekeepers** who know their products the best and can choose the most proportionate tools. However, to alleviate the risk that the gatekeepers undermine the effectiveness of the data portability, the establishment of those mechanisms should be done **in close partnership with representatives of the beneficiaries of those obligations** and under the supervision of the Commission. In reviewing gatekeeper submissions, the Commission could seek input from third-parties (including those representing consumers) and draw on the evidence collected by gatekeepers through A/B testing. The Commission could usefully also set out how it expects gatekeepers to engage with third parties too as explained in the companion paper on DMA process and compliance.

In particular regarding the development of **technical standards that ensure an effective and security and privacy preserving data transfer**, experience suggests that this is best regarded as a process rather than being a discrete event. Therefore, the Commission could play an important role in convening the technical forum in which common standards for APIs and integrated tools would be developed in a manner that fairly balances the interests of all parties, and ensuring that there is an appropriate representation of interests without the process becoming unmanageable.[120] Examples may be drawn from the Australian Consumer DataRight (CDR) initiative, which has also relied on a standardisation body.[121]

This process could seek to build upon work done by the *Data Transfer Initiative*[122] since this already involves a number of gatekeepers, and the Commission would need to ensure that all interests are

[120] DMA, Art. 48 and Rec.96

[121] https://www.cdr.gov.au/

[122] https://dtinit.org/

properly represented and that the resulting outputs do not enable gatekeepers to impose unreasonable costs on others.

Finally, several studies on data sharing arrangements that require the consents of end users place emphasis not only on the ease of using the data transfer process itself but also on the need for policymakers or regulators to **educate and inform users about the benefits of their doing so as well as the control of the risks in terms of privacy and security.**[123] Even if an end-user benefits in terms of being able to switch between platforms, many users may not be aware of their rights. The Commission may ensure that the gatekeeper inform users of their rights and risks or even to inform potential entrants of the opportunities that are available to them.

4.2.3. Non-discrimination

Finally, when there is a relevant benchmark in the internal operations of the gatekeepers, the tools offered by the gatekeepers for data portability to third parties should be non-discriminatory. For instance, in the context of the Revised Payment Services Directive (PSD2 Directive), performance and reliability of the interface used for data portability was measured against the data provider's other consumer-oriented interfaces.[123]

4.3. Relationship with Other EU Legal Provisions

The **data portability obligation of Article 6(10) DMA is complementary to the data siloing of Article 6(2)**; while the latter aims to create a level playing between the gatekeepers and their business users, the former aim to facilitate switching and multi-homing. Both provisions benefit the same business users and a similar scope of data.

The **data portability obligation of Article 6(9) DMA is also complementary to the GDPR**. Both legal provisions have different objectives as the former reduce users switching costs will the latter aims to ensure the self-autonomy of the users. However, Art.6(9) DMA complements Art.20 GDPR[124] by imposing obligations which go further (data should be given continuously and in real time, free tools to facilitate the effective exerciseof data portability …) but only on designated gatekeepers. It is thus important that both the DMA and the GDPR are applied in a complementary manner, through a dialogue between the authorities in charge of the GDPR (the national data protection authorities) and the authority (the Commission) in charge of the DMA within the DMA High-level group.

[123] Ctrl-Shift (2018), p.12: 'Consumers have a lack of know-how and understanding of the digital market, and limited knowledge about their data, how it is used, and how they could use it. This makes the individuals vulnerable to abuse and lacking in the skills to access the opportunity'.

[124] As expressed by Recital 59.

cerre Centre on Regulation in Europe

DMA PROCESS AND COMPLIANCE

RICHARD FEASEY
GIORGIO MONTI

1. INTRODUCTION

As discussed in previous CERRE reports on the Digital Markets Act (DMA), the Regulation provides for a model of compliance which is not based solely on deterrence.[125] While the European Commission is empowered to investigate gatekeepers, identify non-compliance and impose fines, these powers are not expected to be the principal way through which compliance is secured. The expectation is rather that **gatekeepers are encouraged to and will comply by engaging co-operatively with the Commission and with third parties**, including prior to the implementation of measures to comply with obligations.

Moreover, as will be argued below, compliance is viewed as a process whereby the gatekeeper's efforts to comply are expected to be reviewed internally, are assessed by the Commission and third parties on the basis of information available at a particular point in time and which may therefore be adjusted over time and in light of new evidence or experience of their implementation. In most cases, the Commission is not expected to 'certify' that a particular set of measures are compliant at any given point in time and even measures that the Commission does formally find to be compliant must be revisited by the gatekeeper and/or the Commission if they are subsequently found not to be effective.[126]

This approach might be labelled a form of positive regulation whereby: "corporate capacities to self-regulate are used to the maximum extent."[127] This paper considers the implementation of DMA obligations from this perspective and makes recommendations on how this approach might be applied in light of the challenges faced by the Commission in achieving compliance under the DMA.

Our key recommendation is that, given uncertainty about how positive regulation will work in the context of the DMA and the lack of detail about the process in the Regulation itself, the Commission should provide greater clarity at the outset as to how it expects this approach to regulation and compliance to be applied, what it expects of different participants, and how the Commission itself will exercise its powers to encourage as well as to enforce compliance.

Although it might be argued (as the Commission has done in relation to other guidance that might be developed under the DMA) that we should rely upon an iterative process to discover how to best coordinate the various steps to ensure compliance, we think that in this instance it would be better the Commission to provide greater clarity about the compliance process or procedures at the start of the process. This is for the following reasons:

- It would address concerns about how the considerable discretion accorded to the Commission by the Regulation when assessing compliance or approaching enforcement will be exercised.

[125] G. Monti, 'Procedures and Institutions in the DMA', in A. de Streel et al *Effective and Proportionate Implementation of the DMA* (CERRE, 2023).

[126] DMA, Article 8(9), Template Form for Reporting Pursuant to Article 11 of Regulation 2022/1925 (Compliance Report) (9 October 2023), (hereinafter: Compliance Report Template) p. 2 referring to ongoing reporting to the Commission.

[127] R. Baldwin and M. Cave, *Taming the Corporation* (2023, OUP, Kindle Edition) p. 6.

This should build confidence amongst participants, create positive incentives to comply from the outset, and reduce the risk of actions and decisions taken by the Commission being perceived to be driven by (or in fact being driven by) political considerations (given the Commission's dual role) rather than by clear administrative rules.

It should create incentives for gatekeepers and third parties to participate in the process in an appropriate manner and in good faith from the outset, encouraging good behaviour and discouraging practices which might delay compliance or reduce effectiveness.

It should allow gatekeepers to invest in implementing measures with greater confidence that the results will be viewed as compliant by the Commission (provided the gatekeeper has followed good practice) and allow business users or competitors to make investments required to take advantage of those measures without fear that the Commission may later ask the gatekeeper to change them. In other words, it will help to avoid the risk of sunk costs for both gatekeepers and third parties and accelerate the realisation of benefits envisaged by the measures.[128]

It would ensure that the legal principles of good administration, which the Commission is bound by, are articulated in a manner that is clear to all.

The paper is structured in the following way: the legal framework for compliance is set out in section 2. The types of dialogue that the DMA requires and facilitates are discussed in section 3 where we consider the following dialogues: Commission-gatekeeper, gatekeeper-third parties, and Commission-third parties. Section 4 turns to a discussion of how to create incentives for gatekeepers to comply without the threat of sanctions. Section 5 discusses the importance of ongoing compliance and the role of gatekeepers, the Commission, and third parties in achieving this. Section 6 contains our recommendations on the content of the guidance which we propose the Commission provide as soon as possible.

[128] Of course the degree of investment required by gatekeeper and third party beneficiaries varies depending on the obligations. For some prohibitions less is expected than for some obligations.

2. LEGAL FRAMEWORK FOR COMPLIANCE

2.1. Self-assessment

The gatekeeper is responsible for ensuring effective compliance with the obligations in the DMA which apply to it. In addition to this, the DMA sets out two other requirements.

First, **the gatekeeper must demonstrate compliance** by way of a report due six months after designation and annually thereafter.[129] The compliance report is intended to allow the Commission to assess the gatekeeper's conduct. A non-confidential version of this report, which gatekeepers must also produce, is intended to demonstrate compliance to third parties and/or to enable third parties to challenge gatekeepers directly or to signal infringements to the Commission or national competent authorities. The Commission has issued a Template Form for Reporting.[130] This specifies the 'minimum information' that gatekeepers are expected to provide in the report.[131] Section 2 of the Template provides a list of information that must be supplied for each core platform service in relation to which an undertaking has been designated as gatekeeper and includes the following (including information which we highlight in bold relating to dialogue with third parties prior to the adoption and implementation of measures):

- A description of the measures taken;
- Any changes in the customer experience that result from this;
- Changes to the contractual relations between gatekeeper and business users that result from compliance;
- Consultation with end users and business users in the process leading up to the elaboration of the measure as well as during its implementation;
- Identification of alternative measures that were considered and why they were not selected;
- Any action taken to inform end-users and business users of the measures, feedback received and responses to that feedback;
- Any market analysis or testing to estimate the expected impact of the measure and to evaluate the actual impact or evolution of the measures taken on the objectives of the DMA;
- An identification of indicators to allow an assessment of effectiveness;
- Internal systems to monitor effectiveness;

[129] Art. 11 DMA.

[130] Compliance Report Template (9 October 2023).

[131] Ibid., p. 1.

- Where third party access is required the procedures, scope, format and other information relating to such access.

Second, the DMA provides that "[t]he measures implemented by the gatekeeper to ensure compliance with [Articles 5, 6, and 7] shall be effective in achieving the objectives of this Regulation and of the relevant obligation."[132] This requirement presents challenges because it creates an expectation that **the gatekeeper should monitor how effective its compliance measures are and adapt** these as time passes. This is explicitly foreseen in the reporting obligation that "[t]he gatekeeper shall update that report and that non-confidential summary at least annually."[133] The challenges of this requirement are discussed further in section 5. It also creates an expectation that the measures will succeed in contributing to greater fairness and contestability from the outset if properly implemented, which we discuss further in section 3. However, this may be an unrealistic expectation for some obligations which may require further changes after the first compliance report has been issued or after third parties have had an opportunity to engage fully with the measures. Changes might be modest or operational in nature or, in exceptional cases, involve more fundamental revisions to extend the scope or effect of certain measures.

2.2. Commission Specification

The Commission has the discretion to intervene and issue an implementing act specifying how the gatekeeper shall comply with the DMA. This intervention may occur at the request of the gatekeeper or on the Commission's own initiative. Both options are discussed below.

2.2.1. Gatekeeper requests specification

For obligations listed in Articles 6 and 7, the gatekeeper has the option to request that the Commission engages in a process to determine whether the measures that the gatekeeper intends to implement or has implemented to ensure compliance "are effective in achieving the objective of the relevant obligation in the specific circumstances of the gatekeeper."[134]

We consider that requesting a **specification does not stop the compliance clock and that the gatekeeper is still expected to change its conduct and comply on the due date even if it is uncertain as to how to best comply**.[135] However, if the Commission accepts a request to engage in the process foreseen by Article 8 and this results in an implementing act specifying how to comply, then the gatekeeper will be obliged to make necessary changes to abide by the specification.

Nothing in the DMA prevents a gatekeeper from making a request for specification before the date when the obligations it has under the DMA must be implemented.[136] However, we are not aware of

[132] Art. 8 DMA.

[133] Art. 11(2) DMA.

[134] Art. 8(3) DMA.

[135] This is also foreseen in the Template Relating to the Reasoned Request for a Specification Process Pursuant to Article 8(3) of Regulation 2022/1925 (hereinafter Specification Template), section 2.2.

[136] Indeed the Specification Template (Ibid., section 2.2) refers to measures that are intended to be implemented.

any such anticipatory request having been made since designations were made by the Commission in September 2023. Specification requests may also be made lawfully after the date when obligations must be implemented (and we discuss the criteria which the Commission might apply when considering such requests below).

The gatekeeper's request for a specification is without prejudice to the Commission's power to investigate (and possibly sanction) the gatekeeper for non-compliance (assuming this request arrives after the date on which compliance is due).[137] However, we think the **Commission should create incentives for gatekeepers to request specifications by stating that it would not expect to initiate non-compliance proceedings in some circumstances**. Without offering an exhaustive list of those circumstances, we consider the following will be relevant:

- Whether the gatekeeper has engaged with third parties actively and in good faith in designing its compliance approach but differences of view have emerged between third parties;
- Whether the gatekeeper has considered various options on how to comply and seeks advice from the Commission on the best approach, and/or
- Whether the request arrives in good time before compliance is due (i.e. allowing the Commission sufficient time to issue guidance and for the gatekeeper to implement ahead of the deadline).

These are factors that individually and cumulatively should determine whether the Commission decides to engage in specification decisions. In addition, if a compliance report has already been submitted it will also contain information that should inform the Commission's decision, such as whether the gatekeeper has carried out market tests that leave it with some uncertainty about how to best comply or whether the gatekeeper has informed users of the measures taken and has received feedback that is ambiguous or contradictory. If so then the Commission should encourage such efforts by accepting the specification request. The list of users consulted can also be a helpful guide and a limited effort at consultation would count against accepting the request.

Thus a **good faith or 'best efforts' approach on the part of a gatekeeper should be rewarded with a positive response from the Commission to a specification request** whereas a 'last-gasp' request for specification made in the context of third party complaints to the Commission and limited prior consultation by the gatekeeper should not prevent or delay the commencement of infringement proceedings.

The **Commission's discretion** in whether to accept a request to issue a specification is also curtailed by the DMA's requirements that in making this choice it respects "the principles of **equal treatment, proportionality and good administration**."[138] Unfortunately, it is not clear how these principles should be interpreted:

[137] Art. 8(4) DMA.

[138] Art. 8(3) DMA.

- ***Equal treatment*** means, we think, that all requests should be assessed the same way and the same criteria used to evaluate each request. If two gatekeepers seek a specification for the same obligation, equal treatment does not mean that both requests must be accepted: as explained above there should be criteria to determine whether, in light of the prior conduct of the gatekeeper, the Commission will accept or reject. Moreover, equal treatment does not relate here to the content of the specification itself and different measures may be specified for different gatekeepers even if they relate to the same obligation.

- ***Proportionality*** **in this context is less clear**. Again, it relates to the Commission's consideration of the request rather than the measures actually being proposed. One interpretation is to see this requirement as informing a prioritisation policy. For example, it might be that requests which are likely to lead to specifications of relevance to several gatekeepers should have priority over requests which affect only a single gatekeeper or that the Commission will prioritise requests in instances where the harm to third parties might otherwise be large over those where it is less significant. Another is that if the gatekeeper may risk making large investments or changes which are very difficult to reverse, then guidance is more appropriate than if the gatekeeper can more easily modify its implementation measures if they subsequently prove to be non-compliant. Conversely, proportionality might indicate that where multiple complaints from different complainants have been submitted to the Commission and it is clear that the gatekeeper's current measures are causing harm to third parties, then the Commission should reject requests for specification and instead move swiftly to infringement proceedings. This suggests that the application of proportionality to specification requests will be a case-specific exercise. Proportionality may also be relevant to the requirement for the gatekeeper to explain why the request for specification should be accepted. This is reflected in the Template for Specification Requests where the undertaking is expected to explain the reasons it considers the specification process is appropriate to ensure effective compliance.[139]

- ***Good administration*** is about impartiality, fairness, and timely decision-making.[140] This requires quick responses to requests for specification. As no specific timescale is provided for a response to a request, this principle stresses the importance of a prompt response by the Commission. Note that the Commission is expected to produce a preliminary assessment within 3 months of opening proceedings.[141] It would be helpful for the Commission to indicate a timescale for when the Commission will respond to a request for specification, when third party input will be expected, and when a final assessment is expected to be issued.

[139] Specification Template para 2.1.2

[140] Art. 41 Charter of Fundamental Rights.

[141] Art. 8(5) DMA.

2.2.2. Commission-initiated specifications

The Commission may adopt an implementing act for specifications in **two settings: (i) to specify measures required by a gatekeeper in Articles 6 and 7, and (ii) to specify measures to be taken in Articles 5, 6, and 7 when opening proceedings for circumvention**.[142]

While the second instance is clear and the Commission may consider that it is better for it to specify changes in conduct rather than wait for the gatekeeper to discover them for itself, it is not clear what may trigger the Commission to decide to specify measures in the first scenario. One example could arise if the Commission initiates proceedings and finds an infringement, then the gatekeeper is required to 'cease and desist with the non-compliance and to provide explanations on how it plans to comply with that decision.'[143] Upon receiving this explanation, the Commission may decide that it is appropriate to open specification proceedings having regard to the explanation it has received. However, there may be other instances where if the non-compliance decision reveals that the gatekeeper had already identified an appropriate way to comply but had discarded it then it may be appropriate for the Commission to move straight to specification after an infringement is found to minimise the time required for the gatekeeper to comply.

2.2.3. The process leading to specification

The Commission does not start with a blank slate in the specification process. If a gatekeeper asks for specification it must "provide a reasoned submission to explain the measures that it intends to implement or has implemented."[144] When the Commission initiates a proceeding, it will likely be reviewing existing measures or proposals and consider whether these are sufficient or a different course of action is required.

It would be helpful for there to be **further guidance on the content of the reasoned submission which the Commission expects to receive from the gatekeeper**. The existing Template merely says that the gatekeeper should explain the measures it has implemented, or intends to implement, how these are expected to comply with the DMA as a whole, how the gatekeeper will monitor these, what alternatives were considered, and why they were discarded. The problem with this list is that it is a request for the gatekeeper to justify its current policy choice. However, the purpose of a specification request is (when this is being sought by the gatekeeper) to seek assistance because the gatekeeper is presumed to be uncertain about the best measures to achieve compliance. Additional questions that could be considered in guidance from the Commission could include the following:

- Must gatekeepers make a case for having the Commission accept their request by showing that there are for example multiple ways of complying and that it needs guidance as to what is most appropriate?

[142] Art. 8(2) DMA.
[143] Art. 29(5) DMA.
[144] Art. 8(3) DMA.

- Must gatekeepers present the pros and cons of different options?
- Must the gatekeeper demonstrate why the request is 'proportionate'? and/or;
- Could a reason be that in its consultation with third parties, the gatekeeper is unable to find consensus and it is for this reason that it wishes to receive a specification decision from the Commission?

Requiring the gatekeeper to address these points would allow the Commission to better judge whether it is appropriate to accept the request and would also provide information necessary for producing a specification decision.

2.2.4. The content of specification decisions

While proportionality is a key concept when discussing the DMA, it is worth noting that it is only under the framework of Article 8 that the Commission is empowered to specify how a gatekeeper must implement an obligation. Thus, only under this procedure must the Commission ensure that the specification is effective and proportionate and the **burden of showing that the conduct specified is proportionate in this procedural setting is therefore with the Commission**.

In all other cases, it is for the gatekeeper to explain how it proposes to comply. In these settings, a gatekeeper can be expected to use proportionality as a reason to challenge an instruction to do more and may, for example, challenge an infringement decision on the basis that its conduct did not infringe the DMA because it was proportionate. In this case, the **burden of proof is with the gatekeeper**. It follows that a gatekeeper may well adopt measures that are disproportionate in order to avoid further investigation but that this is a risk for it to judge.[145]

A specification is addressed to the gatekeeper and it is expected that the decision will explain why the conduct specified is necessary to ensure effective compliance and also (if applicable) why the Commission considers that the measures already implemented or proposed by the gatekeeper would not be sufficient to comply with the DMA.

2.2.5. The uniqueness of specification decisions

It is worth highlighting that **the only way for a gatekeeper to obtain a formal statement that its conduct complies with the DMA is through a specification decision**. In this procedural context, the Commission may determine either (i) the conduct that the gatekeeper has described is compliant or (ii) the conduct is not compliant and a decision is issued explaining how to comply. Provided the gatekeeper follows the decision then it can assume that it has complied.

The legal security of a specification decision is, however, limited by Article 8(9) which allows the reopening of proceedings in three circumstances:

[145] Except if there is some evidence of maladministration by the Commission. See e.g., Case C-202/06P *Cementbow Handel Industire BV v Commission*, EU:C:2007:255, Opinion of AG Kokott, para 69. For an analogy, see e.g., Case C-441/07 P, *Commission v Alrosa*, EU:C:2010:377 in the context of commitment decisions in antitrust law where the risk of over-compliance is on the parties offering commitments.

- If there has been a material change in any of the facts on which the decision was based;
- If the decision was based on incomplete, incorrect or misleading information, or;
- If the measures specified in the decision are not effective.

A specification decision should therefore include a review clause in which we suggest the Commission could be more specific about the circumstances which might lead to a reopening of the specification. The obvious case is where the specified measure is found not to be effective by the Commission. But the opposite situation might also arise, where the gatekeeper itself asks for the specification procedure to be reopened if it is later discovered that the remedy (or elements of the remedy) is no longer necessary to make markets more fair or contestable and that remedy can be withdrawn. We think it would be helpful for the Commission to elaborate on the criteria and evidence that would be required for the Commission to conclude that aspects of the remedy need to be revisited or that they are no longer required. This may avoid later litigation as to whether the gatekeeper is entitled to ask for a modification of the specification and may save the costs involved in operating this procedure.

No other provision in the DMA empowers the Commission to certify that conduct is compliant. In a non-compliance decision, the onus will be on the gatekeeper to "provide the Commission with a description of the measures that it has taken to ensure compliance."[146] The gatekeeper may ask for a specification as discussed above. It is not clear whether requests for specifications will be denied in instances where the gatekeeper asks for it having been found to be in breach of the DMA. We have suggested earlier that guidance from the Commission on this point and the criteria it would apply in considering such requests would be desirable.

Finally, there are **two other settings where the Commission may determine how far the conduct complies** with the DMA:

- In a *commitment decision* the Commission merely states that "there are no further grounds for action."[147] This does not bind national courts which may decide otherwise.
- In a *market investigation into systematic non-compliance*, the Commission is empowered to impose "any behavioural or structural remedies which are proportionate and necessary to ensure effective compliance with this Regulation."[148] Compliance with this remedy certifies that there is no breach, but this too may be re-opened. Indeed, it seems that a special surveillance regime is in place for gatekeepers who have been found to have systematically failed to comply – Article 18(8) provides for a regular review of the remedies and the power to modify these after a market investigation which finds that they are not effective.

[146] Art. 29(6) DMA.
[147] Art. 25(1) DMA.
[148] Art. 18(1) DMA.

3. DIALOGUES

In addition to the specification process discussed in the previous section, we envisage that **other ongoing interactions or dialogues will need to occur as the DMA is implemented.** We consider these in this section of the paper. They involve interactions between the gatekeeper and the Commission (or national authorities investigating non-compliance pursuant to Article 38(7)) outside of the specification process, interactions between the gatekeeper and third parties and interactions between third parties and the Commission (or national authorities investigating non-compliance pursuant to Article 38(7)[149]).

3.1. Gatekeeper Dialogue with the Commission

The Commission's original proposal for the DMA made reference to a 'regulatory dialogue'. However, this was insufficiently specified and has been omitted from the final version of the text.[150] The **only form of dialogue set out formally in the DMA is that relating to the specification decisions referred to in Article 8** and discussed above.

This noted, there do appear to be **a number of other occasions** where the gatekeeper will be expected to communicate with the Commission:

- **Informally before the deadline for compliance.** In the Compliance Report Template, the Commission states that: '[i]n order to demonstrate compliance as required by Article 8(1) of Regulation 2022/1925, the Commission expects gatekeepers to engage in a regular compliance dialogue with users of the relevant services and with the Commission, including an ongoing reporting to the Commission, in particular when new compliance measures are elaborated and put into place and/or when events impact gatekeepers' compliance with Regulation 2022/1925.'[151] From a legal perspective, it is not clear that gatekeepers can be obliged to communicate with the Commission before the compliance deadline. The DMA does not give the Commission powers to intervene and issue fines or injunctions in the period between designation and the compliance deadline 6 months later. In our view, it would be beneficial for gatekeepers to discuss its proposed compliance measures with the Commission before the deadline but it cannot be obliged to do so. Conversely, below we will argue that there may be instances where an expectation to engage with third parties before the compliance deadline may have some legal consequences subsequently.

[149] In the case of national authorities, the interactions with gatekeepers and third parties will occur only in relation to investigations into non-compliance which they are undertaking. Our assumption is that the approach adopted by the Commission in its non-compliance investigations would be replicated by national authorities so far as possible and having regard to local judicial standards. We therefore propose that the Commission set this expectation in the guidance we recommend and that they consult with the relevant national authorities before doing so.

[150] G. Monti, 'The digital markets act: Improving its institutional design' (2021) 52 European Competition and Regulatory Review 90.

[151] Compliance Template, p. 2.

- In the context of a **non-compliance decision based on Article 29,** a gatekeeper may engage with the Commission immediately after receiving preliminary findings and this may shape the measures it adopts.[152] Alternatively, the gatekeeper can wait until the cease-and-desist order is made at which point it is obliged to provide the Commission with a description of the steps taken to ensure compliance;[153]
- In **market investigations into systematic non-compliance,** the gatekeeper may offer commitments. We would expect that, as in antitrust, a market test of these proposals is used and that there is some discussion between gatekeeper and Commission to refine the commitments. As with the practice found in DG COMP's *Manual of Antitrust Procedures*, we would expect that the Commission should publish an account of how it expects this process to be carried out.

We think a key requirement should be that any dialogue between the Commission (or national regulators) and the gatekeeper is undertaken on **as transparent a basis as possible** (recognising that commercially sensitive information may be involved and that different interests will therefore need to be balanced). This is necessary to ensure confidence in the overall process and to provide third parties with the ability to properly understand and scrutinise the measures taken or proposed by the gatekeeper. The degree of transparency expected may be linked to the specific procedures. For example in a commitment decision, transparency will be linked to ensuring the market testing is effective whereas a request for specification under Article 8(3) will need to allow third parties to understand the basis of the request. This is in addition to the requirement under Article 11(2) to publish a non-confidential version of the compliance report, where we consider the Commission may expect greater disclosure of information than is proposed by the gatekeeper if it considers this necessary for third parties to adequately understand and scrutinise the measures which the gatekeeper has taken to comply. We note the Commission has indicated that it will assess confidentiality claims by the gatekeeper in respect of the compliance report in a manner consistent with the approach taken in antitrust and merger decisions.[154] However, we also note that Article 29 does not envisage the Commission being able to bring a non-compliance decision in relation to the publication obligation for compliance reports in Article 11 and so the Commission could only compel disclosure of information through a normal infringement procedure which is likely to be time-consuming.

As we discuss further below, transparency will also be important in interactions between the Commission and third parties to allow the gatekeeper to understand the nature of any complaints being made against it and to allow all parties to understand the basis and evidence on which the Commission makes its decisions.

[152] Art. 29(3) DMA.

[153] Art. 29(6) DMA.

[154] The Commission indicates this in para 3.1 of the Template for Requests for Specification.

3.2. Gatekeeper Dialogue with Third Parties

In this Section, we consider the circumstances in which gatekeepers should be expected to engage in dialogue with relevant third parties before adopting and implementing measures to comply with obligations in the DMA and the consequences for gatekeepers of doing or not doing so. This reflects Implementation of the various obligations in Articles 5 and 6 will take a number of different forms. **Our view that the DMA introduces an expectation (but not a formal obligation) that gatekeepers engage in dialogue in relation to some measures, whilst others are expected to be 'self-executing'.** Our overall assessment is summarised in the table below and explained further in the rest of this section:

Measures for which any dialogue would be 'voluntary'	Measures for which the requirement of dialogue is unclear and may depend on the interpretation of the obligation itself	Measures for which no prior dialogue may be one indication of non-compliance
Article 5(2), 5(3) 5(4), 5(5), 5(6), 5(7), 5 (8), 5(9), 5(10)	Article 6(5)	Articles 6(3) part only, 6(4), 6(8), 6(9), 6(10), 6(11)
Articles 6(2), 6(3) part only, 6(6), 6(13)	Article 6(7)	Article 7
	Article 6(12)	

3.2.1. Voluntary dialogue

Implementation of the various obligations in Articles 5 and 6 will take a number of different forms. The **obligations in Article 5 and some in Article 6 seem to expect the gatekeeper to alter its own conduct unilaterally and to be 'self-executing'**, either by:

- Ceasing to use data itself in certain ways (Article 5(2) and 6(2)),
- Removing prohibitions on the conduct of business users of the platform (Articles 5(3), 5(4)),
- Removing limitations on the conduct of end users of the platform (Article 5(5) and possibly Article 6(6),[155] or;

[155] Insofar as Article 6(6) does not require the gatekeeper to enable switching between third party applications and services or from gatekeeper to third party applications and services but simply to remove technical or other barriers which might

- Removing restrictions on both business and end users (Articles 5(6), (7) (8) and Article 6(13)).[156]

In these cases, **any dialogue with third parties may be considered by the Commission as part of its compliance assessment, alongside other factors**.

For some obligations, dialogue may be required for some measures but not others. For example, Article 6(3) refers to uninstalling applications on an operating system (OS) and changing default settings. It seems unlikely that dialogue will be required to ensure that users can easily uninstall applications provided by the gatekeeper themselves and it might be expected that the gatekeeper will have incentives to ensure that rival applications can be easily uninstalled. However, Article 6(3) also requires the gatekeeper to develop and present choice screens comprised of both gatekeeper and third party search engines, web browsers and virtual assistants from which the end user will select a default option. In this case, we consider that a dialogue will be required between the gatekeeper and third party user in order to address various technical and operational matters such as eligibility criteria, third party widgets/logos for the choice screen, URLs and other technical information, without which default settings cannot be implemented

3.2.2. Requirement for dialogue uncertain

For **some obligations, the requirement for dialogue is unclear and may depend on the interpretation of the obligation itself**.

For example, ***Article 6(5)*** *prohibits self-preferencing* in ranking and indexing and requires a gatekeeper to apply 'transparent, fair and non-discriminatory conditions to such ranking'. This clearly envisages that the gatekeeper will disclose the criteria it applies when ranking (which it may do in any event to allow users to optimise performance) but it is not clear that the gatekeeper is expected to engage in a dialogue with third parties that might then alter the criteria which it has chosen to adopt. In this case, much turns on whether a decision rule can be said to be 'fair' in the absence of a dialogue with those affected by it, or indeed what the term 'fair' might mean in this context.

currently inhibit such switching. It is possible that dialogue with third parties might be required to identify the relevant barriers, although we would generally expect these to already be well understood by the gatekeeper and for third parties to have informed the gatekeeper about them.

[156] Articles 5(9) and (10) are different in nature and involve the provision of information to advertisers and publishers upon request. Agreement over the format and means by which that information will be supplied by the gatekeeper should be relatively straightforward to achieve and we assume the expectations of advertisers and publishers ought to be similar. There may be a case for some kind of standardisation, as discussed further in section 3.2.2. We also note that whilst Article 5(7) prevents the gatekeeper from bundling other services with the CPS, it presupposes that third parties will be able to effectively supply these other services alongside the CPS if the user chooses not to take the gatekeeper's service. For third parties to be able to offer other services alongside the CPS will require dialogue with the gatekeeper but third party indentfication services, browser engines and payment services are likely 'software applicatons' for the purposes of Article 6(3) and 'services' for the purposes of Article 6(7), both of which we consider will require a dialogue between the gatekeeper and third parties in order for compliance to be presumed.

Article 6(7) raises a different question of interpretation. It requires the gatekeeper to implement technical changes to enable competitors or third parties to interoperate with the gatekeeper's OS or virtual assistants (VA) on the same non-discriminatory basis as the gatekeeper's own hardware and software. In this case, we might expect the gatekeeper to first determine how its own hardware and services interoperate with its OS or VA and then apply the same terms to third parties. That is, nothing in the Article requires the gatekeeper to redesign its own internal interoperability arrangements so as to better accommodate or to specifically benefit third parties. On the other hand, the gatekeeper is required to ensure 'effective' interoperability (echoing 'effective use' in Article 6(4)) and it may be that the provision of interoperability to third parties on the same terms as the gatekeeper currently provides to itself will not enable third party applications to interoperate 'effectively' and that this would be foreseeable if the gatekeeper were to enter into a dialogue with third parties prior to implementing the measures. The Commission will need to take a view based on the specific circumstances of the case.

Article 6(12) illustrates an important point about the steps that a gatekeeper is required to take in order to ensure effectiveness and hence compliance. It requires the gatekeeper to set appropriate terms for business users of its own services. In such cases, engagement with competitors or third parties may not be required but compliance may be more likely if the gatekeeper were to seek views from business users before adopting terms. This would be particularly important if compliance in this context were to reflect an expectation that the gatekeeper is expected to have concluded contracts on compliant terms with potential beneficiaries of the measures before the deadline for compliance (i.e. March 2024) so that their effect would be felt immediately. The alternative interpretation might be that the gatekeeper would publish terms on the compliance date, but that the conclusion of contracts with potential beneficiaries would follow after that.

In order to be able to assess or demonstrate the effectiveness of terms under Article 6(12), we think the Commission ought to expect that gatekeepers engage with third parties prior to the adoption of new contractual terms and not only afterwards, but we recognise that this rests on a particular interpretation of the obligation itself. This suggests that, for at least some obligations, the approach to compliance may depend upon how a particular obligation is interpreted by the Commission (or by the Courts).

Importantly, this point is not confined to Article 6(12). **Many obligations require the gatekeeper to implement measures which also require action to be taken by third parties in order for them to have an effect. The ability of the third party to act and so benefit from the measure will depend upon the gatekeeper first making available certain information or tools**. One interpretation of an obligation is that the gatekeeper is required to disclose the information or tools at the compliance deadline. According to this view, third parties will require some further time to respond and take action themselves before the measure could be said to be capable of having any effect on contestability or fairness. This would only occur later and after the compliance deadline has passed. An alternative interpretation is that the gatekeeper should anticipate the actions which third parties will need to take in order to take advantage of the measure and should provide the information and tools necessary for them to do so sufficiently in advance of the compliance deadline. According to this view, compliance

requires that third parties will benefit from the measure from the outset and that the measure will only be effective if this is the case.

3.2.3. Dialogue as key element of compliance

In some cases, we consider that **prior dialogue with third parties will be essential for effectiveness and hence compliance** and should therefore be regarded as an important factor of the compliance process. This would mean that evidence of a **failure by the gatekeeper to engage in good-faith dialogue with third parties in a timely manner could be one indication, among others, of lack or ineffective e compliance assessment**. This is not of course to exclude the possibility that a gatekeeper may persuade the Commission that it has been able to comply without consultation with third parties, but the Commission's guidance should make it clear that a gatekeeper that relied on such an approach would be taking a greater risk of infringement proceedings.

This could apply in relation to the following obligations:

- Those parts of *Article 6(3)* relating to choice screens, as discussed above.
- *Article 6(4)*, which refers to installing third party app stores and changing default settings and requires users to be able to make effective use of third party applications. We would expect this to necessitate a dialogue between the gatekeeper and third party on various technical and other matters.
- *Article 6(8)*, which requires the provision of performance measuring tools and data to enable advertisers and publishers to undertake verification of their inventory. We would expect dialogue between the gatekeeper and users of the tools and data to be required in order to ensure that they are provided in a manner and format that can be used effectively.
- *Article 6(9)*, which requires the porting of data in real time to third parties and for which technical interfaces and processes between the gatekeeper and third parties of the kind described in the next Section will be required in order to implement the measure.
- *Article 6(10)*, which requires the sharing of data with business users or authorised third parties for the same reasons as for Article 6(9).
- *Article 6(11)* which requires sharing of click, query, and view data, for the same reasons as for Article 6(9).
- *Article 7*, which requires interoperability for messaging services, for the same reasons as for Article 6(9).

The obligations in **Articles 6(8) to 6(11) and Article 7 are not framed in terms of the gatekeeper ceasing some current practices or supplying a service/interoperating with third parties on the same non-discriminatory basis as it already supplies or interoperates with itself. Instead, they envisage the specification and implementation of a new service or functionality** which third parties are then expected to take actions to engage with and to benefit from. In these cases, it is possible and perhaps likely that several different implementation options will be available and that different third parties

will have different views about how the service or technical functions should work or be implemented. Experience from other regulated sectors suggests that in these circumstances, the kind of unilateral implementation by the gatekeeper which may apply for the other obligations, will not be effective.

3.2.4. How should the dialogue work?

In our view and experience, **dialogues between gatekeepers and third parties will need to be carefully structured and governed.** In the Annex to this paper, we discuss in more detail the issues that arise in the implementation of wholesale services in another regulated sector, telecommunication. This is intended to show that the arrangements we envisage are quite different from, for example, the 'DMA industry roundtables' which the European Commission convened in 2022 and early 2023 and involve a more set of structures and processes which are likely to become an important and permanent feature of the DMA landscape.

Third parties who are also competitors (with each other as well with respect to the gatekeeper) may have different or conflicting expectations or requirements as to technical standards, service levels, business processes, or, where appropriate, the commercial terms on which the service is to be provided. A common challenge in these circumstances is, on the one hand, for the gatekeeper to address requests which would otherwise require it to undertake multiple different implementations of the same measure and, on the other hand, to create a forum within which **competitors can co-operate and co-ordinate their interactions with the gatekeeper** in order to narrow down differences and arrive at common positions (without raising competition law concerns). The aim is to have a process which assists the gatekeeper in producing compliant outputs.

Outputs or measures will be compliant if they are effective and, as regards the sub-set of obligations we have identified above, they are more likely to be effective if they are responsive to the requirements and expectations of those who are likely to make use of them. The dialogue process should therefore **allow third parties to provide feedback and views on proposals for implementation before final decisions are taken by the gatekeeper** and in sufficient time before measures are actually implemented. This is so irrespective of whether effective implementation is to be interpreted as requiring third parties to have taken actions to engage with the measure prior to the compliance deadline or to do so afterwards.

Prior dialogue with third parties ought to **reduce the likelihood of subsequent complaints that the measures taken by the gatekeeper are non-compliant** or that they are discriminatory in effect (as against some third parties even if not against all). This risk is reduced (but not eliminated) if potential complainants have been involved in the detailed specification of the wholesale services from an early stage.

When engaging with third parties, we should not expect gatekeepers to engage in unnecessary dialogues or for this to provide a pretext to delaying compliance implementation (recognising that the 6 months compliance deadline following designation may be challenging for some measures and/or some gatekeepers). A **balance needs to be struck between dialogue which may improve the effectiveness of measures** (or reduce the costs for third parties wishing to take advantage of the opportunities they provide) **and dialogue which serves to delay compliance** and so reduces the

effectiveness of the DMA, at least in the short term. It is of course possible that any given dialogue may have both effects.

This means that gatekeepers should be able to refuse to engage with parties who have no clear interest in the DMA obligation in question and refuse to engage further with parties whose views it has already given proper consideration to. On the other hand, third parties with legitimate interests should not be excluded. It will be difficult for the Commission to provide detailed guidance on these matters since they will depend upon particular circumstances, but clear principles can be stated. In this context, it is important to stress that **consumer or end user representatives should be presumed to have an interest** in all obligations since consumers are expected to be the ultimate beneficiaries, although we recognise they may be in a better position to contribute in some instances than others in practice. It appears that the Commission will monitor who the gatekeeper consults with through the compliance reports which require among others a list of parties consulted.[157]

Finally, we recognise that a dialogue with third parties may not produce any consensus as to the measures to be adopted or the way in which they are implemented. We explained earlier how we think the Article 8 specification process can play an important role in these circumstances. However, **responsibility for compliance and for adopting measures to achieve it ultimately rests with the gatekeeper, who is free to reject particular requests from third parties or to favour its own approach over those suggested by other parties**. The gatekeeper may have information that individual third parties, or that third parties collectively, do not have (although third parties will also have information that the gatekeeper does not otherwise have). Again, we would expect the gatekeeper to explain its decisions in the compliance report.

3.2.5. Standardisation

The issues may become more complex if several gatekeepers were to be designated in relation to the same core platform service (CPS) and so be required to supply similar wholesale services to the same competitors or business users. In these circumstances, there may be a **benefit in having common standards and processes amongst gatekeepers so that third parties can interact with multiple gatekeepers in the same way in relation to the same wholesale services**. This might, for example, allow competitors to more easily aggregate data that they obtain from multiple gatekeeper sources or to use standard APIs to access the same OS or hardware functions operated by different gatekeepers rather than having to develop different versions of the application for each gatekeeper. This might also aid the Commission in assessing compliance or in comparing output indicators (which are the subject of a separate CERRE paper).[158]

[157] Compliance Template , para 2.1.2(ii)(j).

[158] In this context, a question may arise as to whether the Commission can require several gatekeepers to align their measures, whether through formal standardisation or via the specification process or the enforcement process, so as to enable third parties to more effectively engage with them (e.g. by avoiding the need of third parties to have different processes when engaging with different gatekeepers). It might be argued that any measures taken by a particular gatekeeper will be more effective if they align with measures taken by other gatekeepers (in relation to the same obligation). On the other hand, it is difficult to see how the assessment of compliance by one gatekeeper can be contingent upon the actions of another gatekeeper.

In these circumstances, it may be that a dialogue between gatekeepers is required, or develops, and/or that several gatekeepers engage with third parties collectively rather than, or as well as individually.

We recognise that standardisation raises a host of issues and that there is no formal provision or requirement in the DMA that would require a gatekeeper to participate in a sector wide approach of this kind or to adopt industry standards. **Article 48 allows the Commission to "mandate European standardisation** bodies to facilitate the implementation of the obligations set out in this Regulation by developing appropriate standards." However, it is not clear what conditions are required for the Commission to deem it 'appropriate and necessary' to trigger this. For example, some technical features may be more suitable for standardisation than others and standardisation of some features may yield greater benefits than others. There is also a question of timing: standardisation that occurs after gatekeepers have already implemented their own proprietary measures to comply with obligations will likely involve costs for both gatekeepers and third parties, whereas standardisation that precedes implementation will likely involve significant delays in compliance. These trade-offs are well understood but not easy to resolve. It may be preferable for the gatekeepers themselves to request (either individually or collectively in relation to a particular CPS and obligation) that the Commission mandates standards and it would also be open to third parties to do so. Gatekeepers may prefer the use of standardisation bodies to avoid antitrust liability should they co-operate independently instead and might consider that a standardisation body gives greater legitimacy to the final outcome.

Furthermore, Article 46 allows the Commission to adopt implementing acts for "the form, content and other details of the technical measures that gatekeepers shall implement in order to ensure compliance with Article 5, 6, or 7."[159] This is a potentially important aspect of the DMA compliance process where further clarity would be useful.

3.2.6. Role of Articles 5(6) and 13(6)

We noted above that the **dialogue between the gatekeeper and third parties is intended to allow a range of technical and non-technical questions to be resolved amongst the interested parties without recourse to the regulator, who is unlikely to be well placed to do so. At the same time, consensus or agreement may not always be possible and intervention by the regulator may then be required** (for example, via the Article 8 specification process or infringement proceedings).

Here there is a difficult balance to be struck between on the one hand ensuring that third parties contribute to a meaningful (i.e. two-way) dialogue by, for example, disclosing information which may assist the gatekeeper (as well as requiring information from the gatekeeper) or giving the gatekeeper an opportunity to resolve issues before the Commission intervenes. On the other hand, the dialogue with the gatekeeper cannot be used to exclude or render the Commission ineffective as a regulator or otherwise to allow the gatekeeper to exploit its market position.

[159] In so far as we are aware, there is no intention on the part of the Commission to do so at this point.

Article 5(6) of the DMA could be seen as seeking to address this issue, at least to some extent. It has two functions. On the one hand, it is designed to ensure business users and end users are able to make complaints to the Commission (or national authorities) when they are dissatisfied with the conduct of gatekeepers and that the gatekeeper is not able to impose gagging clauses upon them. The first sentence of Article 5(6) clarifies that the gatekeeper cannot directly forbid such complaints, which suggests that any contract term that places limits shall be removed.[160] But it is wider than that as it also forbids any indirect restrictions on business users raising non-compliance issues. It should be read together with Article 13(6) by which the gatekeeper shall not degrade the conditions or quality of any of its CPS provided to business users who avail themselves of the DMA (e.g., as a form of retaliation against a user who has complained to the Commission about the gatekeeper).

Second, it allows (but does not require) gatekeepers to establish an alternative dispute resolution mechanism or any other complaint-handling system to resolve concerns by business users. This is another opportunity for dialogue and may help address difficulties in the design of a remedy that might affect some business users in unexpected ways.[161] A specific obligation to provide an alternative dispute settlement mechanism is found in Article 6(12) of the DMA.

The scope of Article 5(6) is potentially quite wide. In terms of scope end-users and business users cannot be prevented from raising any issue pertaining to 'relevant Union or national law'. Its personal scope is also quite broad. Article 2(21) defines a business user as 'any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users.' This means that the gatekeeper's obligations in this article apply both to business users who engage directly with a gatekeeper and those who do so indirectly. For example, if a new search engine were to emerge then Article 5(6) would apply to the relationship between a gatekeeper (e.g., the provider of an Operating System) and the search engine, but it also applies to advertisers who wish to use the new search engine.

A possible safeguard against concerns that gatekeepers may seek to limit the ability of third parties to refer to the regulator (either by threatening retaliation or by offering positive inducements or preferential terms) is again **to ensure that the dialogue between the gatekeeper and third parties is as transparent as possible** and for the Commission to indicate that bi-lateral engagements or bespoke arrangements between the gatekeeper and individual third parties should be avoided wherever possible.

[160] see also recital 42 DMA

[161] This is comparable to the obligations found in the P2B Fairness Regulation. See European Commission, Report on the first preliminary review on the implementation of Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services SWD (2023) 300 final, suggesting these measures have had limited impact so far. Article 5(6) may impose additional requirements on gatekeepers.

3.3. Commission and Third Parties

3.3.1. Channels for the dialogue

The Commission will engage with third parties about their expectations for implementation. Formally, the following channels exist:

- **At any time**, parties may inform the Commission or national competent authorities about the conduct of gatekeepers. Both institutions retain 'full discretion' as regards the measures to take and have no obligation to follow up on the information.[162]

- **During a *specification decision*,** third parties may comment on the preliminary findings because the Commission must provide a non-confidential summary of the case and the measures it considers taking or that the gatekeeper should take.[163] Here, there is a compromise between speed and consultation: third parties are only entitled to one round of comments. This deprives them of the opportunity to respond to any change of position that the Commission seeks to take upon receiving their information.

- During a **market investigation into *systemic non-compliance***,[164] third parties have a say when the gatekeeper offers commitments: they receive a non-confidential summary of the case and the main content of the commitments. As with specifications, they are allowed to comment only once in order to accelerate the process. More generally when it comes to third parties in commitment decisions, if the case law in antitrust is followed, the Commission cannot accept commitments that interfere with existing third party rights.[165]

There is no express provision for third parties to be heard **when a *non-compliance decision* is made**.[166] Here the gatekeeper communicates the changes in conduct to the Commission. It **is arguable, that if third parties are the direct beneficiaries of the DMA, then they should have an opportunity to be heard even if this is not expressly provided for,** because it is a general principle of EU Law. The Court has recognised this right in the past, although in a different setting. In *Air Inter,* for example, the Commission challenged French legislation which infringed European law but which conferred a benefit to Air Inter. It was held that Air Inter as a direct beneficiary of the French rules had a right to be heard.[167] From this, one may elicit a general principle by which even absent a statutory provision, direct beneficiaries of EU Law should also be able to be heard in proceedings that affect them.

3.3.2. Governance of the dialogue

As with engagement between third parties and the gatekeeper, the **Commission will need to ensure that its engagement with third parties contributes towards, rather than delaying, compliance with**

[162] Art. 27 DMA.

[163] Art. 8(6) DMA.

[164] Third parties are also able to participate in market investigations for designating gatekeepers as they may receive a request for information under Art. 21 DMA. We do not deal with designation in this paper.

[165] Case C-132/19 P, *Groupe Canal+ v Commission*, EU:C:2020:1007.

[166] Art. 29(4) DMA: the Commission may consult third parties.

[167] Case T-260/94, *Air Inter v Commission*, EU:T:1997:89.

the DMA. It is important, for example, that third parties should normally **exhaust the dispute resolution processes** that we envisage will be part of the structured dialogue between the gatekeeper and third parties before they complain to the Commission. However, this should be without prejudice to the business user bypassing or exiting that process and explaining to the Commission or a national authority why the gatekeeper's internal dispute resolution system is insufficient. It is also important that both parties engage properly in the structured dialogue (and in the dispute resolution process offered by the gatekeeper) rather than engaging in strategic behaviour that is intended to produce a particular regulatory outcome (including delaying implementation).

The Commission has **discretion in allocating its resources and in deciding how to respond to complaints that it receives from third parties** and has considerable experience in doing so in other contexts.

We have already made proposals about the Commission's role in **ensuring adequate disclosure to third parties** (e.g., in the non-confidential version of the compliance report but potentially at other stages in the compliance process as well) to enable them to comment constructively and meaningfully upon the actions being taken or proposed by the gatekeeper or their likely effects. The purpose of such disclosures will depend on the procedure being used: in cases of commitment decisions for example, a market test requires that interested parties see what the gatekeeper proposes and the gatekeeper is able to observe and respond to the interventions of third parties. Conversely, Article 34(4) governs access to third party information in the Commission's case file to allow the gatekeeper to understand the case against them in infringement proceedings but it may also be useful to encourage third parties to disclose information to parties other than the Commission at other stages in the compliance process so as to facilitate dialogue between them.

We have also said that the Commission should be **transparent in its dealings with third parties in the same way as it is in its dealings with gatekeepers**. That said, we also recognise that third parties that are also business users (or even competitors or potential competitors who are not) may be reluctant to engage with the Commission if they fear (legitimately or not) that disclosure of their identity or the nature of their complaint might result in retaliation by the gatekeeper. In these circumstances, we think it will be important and helpful for the Commission to provide **further guidance on how (and when) third parties should engage with the Commission and how the Commission will ensure transparency whilst also protecting third parties from risks of doing so** (i.e. in addition to the provisions in Article 34(4) which relate to the protection of business secrets rather than protection against retaliation).

4. INCENTIVES

4.1. Incentives for Gatekeepers

As we explained earlier, **the DMA does not oblige gatekeepers to engage with third parties who may be affected by measures to comply with obligations**. Article 28(4)(d) requires the "Compliance Officer to [co-operate] with the Commission for the purpose of this Regulation" but does not explain what this might mean in practice. The DMA contains deadlines for compliance (6 months from designation) which apply irrespective of the approach to compliance taken by the gatekeeper.

Other aspects of the DMA **allow the gatekeeper to exercise a degree of discretion** in deciding how to approach compliance with the DMA's obligations. For example:

- *Article 8(3)* contemplates that gatekeepers may request guidance as to whether a particular set of measures which it has implemented or which it proposes to implement to comply with Articles 6 and/or 7 are deemed by the Commission to be effective. If the Commission considers that they are not, the Commission can specify other measures that would be required to ensure effectiveness. Thus, gatekeepers may differ in their approach over whether or not to submit such a request to the Commission, when to do so (before or after measures have been implemented), and whether, if the Commission suggests additional measures are required in its preliminary view, it waits a further 3 months until the final decision or takes pre-emptive action to implement the Commission's proposals.

- If the gatekeeper is subject to a preliminary finding of *non-compliance* under Article 29(3) the gatekeeper may decide to adopt the measures which the Commission considers it should take to ensure compliance and, having done so, it may be that the Commission will decide not to adopt a non-compliance decision or to adopt a decision but not to impose a fine or to impose a lesser fine. There is no guidance in the DMA itself as to the implications of a gatekeeper seeking to pre-emptively resolve non-compliance concerns and, unlike the commitments under Article 25 discussed next, it is not expressly contemplated that gatekeepers would seek to resolve individual (as opposed to systemic) non-compliance proceedings through pre-emptive action.

- If the gatekeeper is subject to a market investigation under Article 18 for *systematic non-compliance*, it may decide to offer commitments under Article 25 to resolve matters without the Commission proceeding to a decision or other actions such as the imposition of additional behavioural or structural remedies. Gatekeepers will therefore have some discretion in first deciding how much risk to assume of being found non-compliant on at least three occasions within eight years (this being the trigger for an Article 18 investigation) and, if they have been, whether or not to offer commitments with a view to closing the investigation.

The **Commission itself has considerably greater discretion in deciding how to engage with a gatekeeper**.[168] For example:

- It can decide whether or not to accept a request from a gatekeeper for *guidance* on the effectiveness of measures under *Article 8(3)* "respecting the principles of equal treatment, proportionality and good administration";
- It can decide whether or not to provide guidance to a gatekeeper under Article 8 (2) without having received a request from the gatekeeper to do so;
- It can decide whether or not to investigate *non-compliance* under Article 20;
- It can decide on the level of *fines* to be imposed in the event of a finding of non-compliance under Article 29;
- It can decide whether or not to investigate *systematic non-compliance* under Article 18 (always provided that the gatekeeper in question has failed to comply on at least three occasions in the preceding eight years).

Given the options available to the gatekeeper and the discretion available to the Commission in deciding how to respond to requests from or actions taken by the gatekeeper at various stages in the process, it is clear that at least some **differences in approach to engagement between the gatekeeper and the regulator are both possible and likely** to be taken. It is also possible the same gatekeeper may decide to adopt different approaches in relation to the implementation of different obligations given different benefit/cost calculus.[169]

With this in mind, the **Commission should consider how to incentivise co-operative behaviour on the part of the gatekeeper**. This should be intended to yield benefits for the gatekeeper, third parties and regulator: more predictability and potentially lower costs of implementation for the gatekeeper (with measures that are more likely to reflect their views and less likely to be unilaterally imposed by the Commission), more rapid and effective implementation, and lower cost for the regulator. In order to provide incentives, the Commission will need to reassure gatekeepers that certain forms of conduct

[168] We exclude Articles 9 and 10, which allow the gatekeeper to request and/or the Commission to consent to the suspension or non-application of measures to comply with some or all aspects of obligations on the basis that we would expect this to arise only in exceptional and specific circumstances rather than part of a gatekeeper's overall approach to implementation.

[169] For example, some may seek a more co-operative or collaborative engagement with the regulator and/or with third parties who will be affected by the measures the firm proposes to adopt, whilst others may engage less with the regulator and may not engage with third parties at all. The choice of approach is likely to be influenced by the regulated firm's perceptions of the likely outcomes, in terms of substantive measures taken and risks of fines or other costs during the process but also in terms of the time that will be required to implement the measures. For example, a regulated firm may adopt measures which fall short of compliance in the expectation that further steps will delay the implementation of effective measures and that this can be achieved without financial penalty. The regulated firm can be expected to weigh upon the financial and other benefits of non-compliance or, more likely, delayed compliance against the potential financial and other costs.

will be assessed in certain ways, both positively and negatively. This reassurance will need to be provided at the outset if it is to influence the gatekeepers' behaviour and approach to implementation, as it is intended to do. Having done so, it will also obviously be important that the Commission's subsequent conduct is consistent with the guidance it has provided.

Thus, for example, the Commission could clarify that:

- The Commission will take a gatekeeper's record of implementing measures in a timely and effective manner (i.e., its record on implementation more generally) when considering specific requests from gatekeepers for specification under Article 8.[170]
- The Commission might take the gatekeeper's approach to disclosure, or the quality of its compliance report, into account when considering requests from gatekeepers under Article 8 or when assessing compliance generally on the basis that greater disclosure will enable better scrutiny by third parties.
- As already explained, the Commission will take certain factors into account, such as whether and the extent to which the gatekeeper has proactively and in good faith engaged with third parties in developing its measures to comply, when assessing their effectiveness. Thus, for certain measures, the Commission could state that they will presume non-compliance if the gatekeepers have declined to consult with third parties (and taken their input into account) before implementing measures, whereas, for other obligations, evidence of engagement may form part of the assessment but would not be determinative. Any presumption in relation to any obligation would of course be rebuttable by the gatekeeper demonstrating that its compliance is effective.
- The Commission may take the extent to which the gatekeeper can show third party preferences are reflected in the measures the gatekeeper has chosen to adopt when assessing their effectiveness. This may include an assessment of any third party engagement plan that the gatekeeper has decided to publish on a voluntary basis.[171]
- The Commission may consider the extent to which third party complaints were resolved by the gatekeeper through its own dispute process when deciding whether to respond to complaints submitted by third parties to the Commission, or when assessing compliance of the measures to which those complaints relate.
- The Commission may consider early implementation of measures in response to preliminary findings of non-compliance under Article 29 when deciding whether or not to proceed to a final decision and/or to impose a fine and/or the level of such a fine.

[170] This would be in addition to the guidance we propose that would explain how the Commission will assess requests for specification and what they should contain. The proposal here is not intended to assist gatekeepers in making requests, but to encourage effective compliance with other obligations that can be implemented without specification.

[171] This goes a bit further that what is provided on the Template for Compliance section 2.1.2(ii)(i) and (l) (p. 4).

We note that it is **quite common for such factors to be taken into account by a regulator and for a regulatory regime to include incentives which are intended to encourage particular modes of engagement** – although we also recognise there are differences between the DMA and other regulatory regimes. For example, the energy and water regulators in the UK both require regulated firms to undertake formal consultative exercises with consumers (or their representatives) and other stakeholders when developing budget proposals which the regulator will then assess for the purposes of setting controls for retail or wholesale prices. Proposals which demonstrate effective engagement with customers will be accorded a higher rating than proposals which do not (other factors being equal) and may contribute to the fast tracking and early settlement of regulation for some regulated firms but not others.[172] Early settlement in this way offers both financial and reputational benefits for those firms that obtain it.[173] Similarly, many regulators and competition authorities, including the Commission, will take account of the extent of co-operation (beyond the legal minimum) in proceedings prior to the finding of non-compliance when assessing the level of the fine.[174] This again provides financial incentives to co-operate and ensure lower costs for all concerned and faster resolution.

Similarly, firms often advocate forms of co-regulation under which firms are collectively left to determine how to implement and enforce measures rather than being subject to a statutory regime which has been designed by the regulator. This may offer greater autonomy to industry participants and may produce better outcomes at a lower cost. However, regulators will generally accept such approaches only under certain conditions and may impose statutory solutions in the event that industry participants fail to deliver the outcomes that have been promised.

4.2. Incentives for Third Parties

We expect that **most third parties will have strong incentives to engage with the gatekeeper and the Commission to ensure that implementation is as effective as possible**. We have also seen that there are opportunities for third parties to participate in informing the way in which gatekeepers comply with their obligations under the DMA, either formally at particular points in the process or as a participant in the dialogue between third parties and the gatekeeper which, as explained earlier, we expect to be presumed for the effective implementation of some of the obligations.

We already noted that the **ability of third parties to engage will be influenced by their access to information about the measures the gatekeeper** has taken or proposes to take to comply, whether provided within the structured dialogue or the compliance report which will, amongst other things, report the outcome of that dialogue. We have also said that engagement, and particularly complaints to the Commission by third parties, may be influenced by fears of adverse commercial consequences, such as retaliation.

---

[172] See https://www.ofgem.gov.uk/sites/default/files/docs/2017/01/consumer_engagement_in_the_riio_process_final_0.pdf.

[173] See https://www.nera.com/content/dam/nera/publications/newsletters/energy-regulation-insights/NL_ERI_Issue_42_0116.pdf.

[174] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006XC0901(01), Clause 29.

While engagement by well-informed third parties will often be valuable and can assist the Commission in overcoming information asymmetries in its engagement with the gatekeeper, the Commission should anticipate that **some third party responses may not always be inspired by the public interest or the wider objectives of the DMA, but by narrower commercial interests**. This is not a new challenge for a regulator or antitrust authority or one that is specific to the DMA and the Commission is well-practised in assessing third party submissions. However, transparency in dealing with a third party may also assist here.[175] Third parties may be reluctant to be revealed as purveyors of exaggerated or unsubstantiated claims and the gatekeeper or other third parties have a better opportunity to rebut them if the dialogue between the third party and Commission is as transparent as practicable.

[175] CMA, Market Studies and Market Investigations: Supplemental guidance on the CMA's approach (2017) para 3,32. The CMA also involves third parties in oral hearings.

5. MONITORING AND ADJUSTING

One of the distinctive features of the DMA is that for gatekeeper conduct to be compliant, it must be assessed as being effective in achieving the overall objectives of the DMA (i.e., making markets more contestable and removing unfairness), as well as the specific objectives of the relevant obligation (some of which focus on contestability others on fairness, some on both objectives). This is an obligation to provide a result on the market. Such obligations may be found in some contracts (e.g., where a party commits to deliver goods on Friday, then there is a breach if delivery is delayed) but it is unusual to find this obligation in regulation. The political reason for this may be concerns that antitrust remedies imposed in the past had not been effective.[176]

In line with the recommendations in the other parts of this paper, we suggest that one way of ensuring that conduct is effective is to **treat a gatekeeper's compliance effort with respect to some obligations as an ongoing work-in-progress**, provided that the gatekeeper engages with the Commission and third parties in modifying its conduct when appropriate to do so. In other words, while effective compliance will be expected on the day on which the obligations become binding 6 months after designation, the expectation will also be that gatekeepers may identify (on their own or after prompts from third parties) improvements in light of subsequent experience of implementing the measures and observing their effects. This is implied in the tasks of the compliance officers which include organising, monitoring and supervising the measures of the gatekeeper.[177] It is also implied in the reporting obligations in Article 11 as specified in the Compliance Report Template.[178] Taken together, this suggests that compliance is a dynamic exercise during which the Commission will make assessments and reassessments at particular points in time.

For gatekeepers, this means that they are expected to keep the measures they take under review and monitor their effects or effectiveness. For example, if third party business users are regularly complaining about certain terms or certain types of conduct then the gatekeeper is expected to respond promptly. A prompt and effective response following dialogue with third parties should generally enable the gatekeeper to avoid a Commission investigation into past non-compliance.

The degree to which gatekeepers will be expected to review their compliance with obligations will depend on a variety of factors but generally speaking, **the discharge of some obligations is likely to be satisfied with a one-time change, while for others measure to improve compliance in light of new information will be necessary**. To give two examples:

- Securing end-user consent for data collection under Article 5(2*)* is likely to be one example of ongoing work-in-progress where the best choice architecture cannot be easily determined *ex*

[176] Monti, Taming Digital Monopolies: A Comparative Account of the Evolution of Antitrust and Regulation in the European Union and the United States (2022) 67(1) Antitrust Bulletin 40.

[177] Art. 28(5)(b).

[178] For example this requires a report on "any internal systems and tools used to monitor the effectiveness of the measure and the output of such internal systems and tools (section 2.1.2(ii)(s).

ante.[179] Moreover, as users' understanding changes if more information is provided this may well mean that less effort is needed by the gatekeeper to secure consent. In this context, a good faith effort by a gatekeeper to provide a clear consent form should not be sanctioned if, after a trial of several multiple months, it is found that end-users remain unable to understand what choices they are making.

- Conversely, building a data silo to comply with Article 6(2) is likely to require a one-time implementation where the gatekeeper determines the relevant data, data uses and authorised and unauthorised data uses and users and builds a system that prevents forbidden uses of data. This too can be regularly tested for errors by the gatekeeper to avoid risks that business user data is utilised to compete against them, but here the design should be relatively clear and fewer errors should be tolerated.

We recognise that this approach is not risk-free as gatekeepers may refuse to improve upon their compliance efforts in light of third party feedback. This risk would be managed by the capacity of the Commission to escalate and impose punitive measures when it comes to gatekeepers who do not make good faith efforts to comply and by exercising its discretion in other ways, as discussed earlier. The Commission also has powers to impose interim measures, and third parties can use courts to enforce their rights.

This approach also impacts the Commission and third parties. **The Commission has several channels at its disposal to secure compliance and to monitor gatekeeper conduct**: in addition to the reports, the Commission may take additional steps to monitor gatekeepers, appointing external experts if necessary,[180] and working with compliance officers.[181] We have also suggested earlier that the Commission may be an observer in the structured dialogues between the gatekeeper and third parties, which will provide the Commission with early visibility of the measures the gatekeeper is proposing to take and is consulting upon with third parties and the concerns that third parties may have in relation to those proposals. This should allow the Commission to exercise influence and indicate its position if the gatekeeper were to pursue one approach rather than another before the gatekeeper has taken any final or irrevocable decisions and in advance of any subsequent intervention following a complaint from third parties or the opening of an infringement proceeding. This should therefore have benefits for the Commission (greater effectiveness and/or earlier intervention) and the gatekeeper (less risk of sunk costs and fines). This should not be seen as preventing the Commission from initiating proceedings for non-compliance if and when a gatekeeper is not responsive to the way the Commission expects it to comply.

[179] This is a measure for which we do not consider gatekeepers need to engage in dialogue with third parties, but this does not mean the gatekeeper will not need to consider feedback and new information about effectiveness which it will be able to obtain for itself.

[180] Art. 26 DMA.

[181] Art. 28(5)(d) DMA.

Third parties will also have access to information that allows them to observe how gatekeepers have behaved or are behaving (the non-confidential report) but, as or more importantly, the dialogues we propose would mean that many will also be **interacting directly with the gatekeepers prior to any measures being implemented**. To the extent that proposals give rise to concerns, they can seek informal resolutions, first with the gatekeeper themselves and then the Commission, failing which they can trigger the Commission's more formal enforcement powers.[182] Again, this should benefit all parties by improving effectiveness, reducing sunk costs and lowering the overall regulatory burden.

[182] N. Gunningham and D. Sinclair, 'Smart Regulation' who describe this as a process where you shift from one side of a regulatory pyramid (3rd party pressure) to another (government enforcement).

6. RECOMMENDATIONS FOR THE COMMISSION

The initial set of CPS and gatekeepers were designated by the Commission on 6 September 2023. We understand that some of the gatekeepers that have been designated have engaged with third parties to some degree, but others have not. Establishing the working groups and other features of a 'structured dialogue' will take some time and it may not now be feasible to do so (or might jeopardise other steps being taken) prior to the implementation deadline in March 2024.

Although we recognise these concerns, we think it would be unfortunate if the effect of the DMA timelines was to deter gatekeepers from engaging proactively with third parties as we propose or was instead to encourage them to act unilaterally and without consultation during this initial period. The Commission should consider steps to avoid this, or at least to encourage the kind of dialogue we propose in the longer term.

The **Commission could do this by clarifying its stance on the issues we have discussed in this paper and which we summarise below. Our suggestion is that many of these issues can be set out in a Best Practice document, which can be revised regularly**, as experience in implementing the DMA develops over time.

First, there are several aspects of the **specification process where the Commission enjoys discretion and where guidance would be helpful** (in addition to the information to be provided by the gatekeeper when submitting a request which has been detailed in the recently published Template for specification dialogue request[183]):

- How the Commission will assess requests for specifications from gatekeepers, and what 'equal treatment', 'proportionality' and 'good administration' mean in this context.
- How long the Commission will required to undertake its assessment of the request.
- Whether a gatekeeper can submit a request for specification after having been found to be non-compliant with an obligation and how the Commission would approach its assessment of such a request.
- How long the Commission will require to issue a final decision on specification.
- The role of third parties in the specification process.
- The circumstances in which a gatekeeper may request the Commission to revisit a specification decision which it has previously adopted and the evidence required in such a request.

[183] https://digital-markets-act.ec.europa.eu/document/download/b034f7c4-c877-420c-87fa-0e69f8aea522_en?filename=Article%208%283%29%20DMA%20Template%20%28request%20for%20specification%20dialogue%29_1.pdf.

- The circumstances in which the Commission may itself revisit and amend a specification which it has previously adopted.

In addition, the Commission should provide guidance on **how it will engage with gatekeepers and third parties in a transparent manner.** As part of this, it should elaborate upon its expectations regarding claims for the confidentiality of information**,** both in relation to the compliance report that is to be published by the gatekeeper and in relation to the provision of information by gatekeepers and third parties more generally. The Commission should explain how it will address concerns that disclosure by third parties may facilitate retaliation by a gatekeeper and thereby deter dialogue.

The Commission should clarify its **expectations on engagement or 'structured dialogues' between gatekeepers and third parties** in relation to implementation. In doing so, we suggest:

- It distinguishes between obligations for which engagement is not key in the compliance assessment and may not be required at all and obligations for which engagement is likely to be essential; our proposals in this regard are summarised in the table in section 3.
- It should clarify its expectations on whether third parties should already have been able to take actions prior to the compliance deadline so that those measures have an effect on the market from that date or whether it is sufficient for the gatekeeper to make the opportunity available from that date but that any effects would be seen later and only once third parties had taken the actions (such as ordering services, providing information or agreeing terms) after the compliance deadline.
- It should clarify the meaning of Articles 6(5) and 6(6) and whether or not, in light of this, compliance will necessitate a prior dialogue
- It clarifies that gatekeepers are expected to determine the best form of engagement with third parties and to inform or provide guidance to enable any third party to engage effectively (including timelines) with the gatekeeper on a non-discriminatory basis.
- It clarifies the Commission's expectations of third parties when they engage in dialogue with the gatekeeper (including normally exhausting alternative dispute resolution mechanisms before complaining to the Commission and not engaging in strategic behaviour).
- It highlights some of the issues which such engagement between gatekeepers and third parties is likely to be best placed to address, including the production of a reference offer (formally required by Article 7 but likely also practically necessary to implement Articles 6(7), 6(9) to (11) effectively). The contents of such an offer will likely need to address, inter alia: ordering, fault reporting, testing, forecasting, dispute resolution and other operational matters that are better resolved by dialogue between the gatekeeper and third parties than intervention by the Commission.
- It clarifies that the dialogue between gatekeeper and third parties cannot exclude the Commission from using its powers to intervene to ensure compliance and explains the

relevance of Articles 5(6) and 13(6) in safeguarding the interests of third parties in this context.

- It clarifies that the dialogue should be designed to allow both the Commission and third parties to influence the measures that will later be adopted by the gatekeeper so as to improve their effectiveness before they are adopted instead of relying only upon complaints and intervention after they have been adopted.
- It outlines some of the issues which the Commission considers will be important to address before embarking on an effective structured regulatory dialogue (and to which the Commission would therefore regard when assessing any measures which result from that dialogue) including:
    - Criteria for participation in the dialogue
    - Arrangements for administrative support and recordkeeping
    - Relationship between the dialogue and engagement by gatekeepers and third parties with the Commission and/or engagement by the Commission in the dialogue and
    - The role of competition law.

The Commission should explain that it will seek **to encourage 'co-operative conduct'** on the part of gatekeepers which is likely to contribute towards effectiveness and what it means by this. Examples of such conduct might include:

- Early implementation of measures following a preliminary specification decision or a preliminary non-compliance decision.
- Proactive and good faith engagement with third parties and publication of guidance for third parties on how to engage with the gatekeeper.
- Prompt resolution of third party complaints by the gatekeeper, either through the gatekeeper's dispute resolution process or by other means.
- Evidence of third party views and interests informing the measures which the gatekeeper has adopted or proposed to adopt
- Extensive voluntary disclosure in the non-confidential version of the compliance report
- High-quality compliance reports which allow third parties to fully engage in the assessment

The Commission should clarify how it will take 'co-operative conduct' by the gatekeeper (vis-à-vis both the Commission and third parties) into account when:

- Assessing the effectiveness of particular measures and deciding whether or not to commence infringement proceedings.
- Deciding whether to accept or reject a request for specification.
- Deciding whether to proceed to a final non-compliance decision.
- Determining the level of any fines or whether to impose a fine at all.

The Commission should provide more guidance on the **procedure for commitments in an investigation into systematic non-compliance** so gatekeepers and third parties are aware of what is expected of them when making commitments or in assisting the Commission in assessing them.

The Commission should explain the **circumstances under which it might expect to exercise its standardisation powers** under Article 48, including in response to a request to do so from a gatekeeper.

The Commission may explain that **its assessment of compliance may depend not only on the conduct of the gatekeeper in developing and implementing measures initially but also upon conduct over time.** It should explain that some obligations may require an iterative process in which measures change so as to become more effective in light of new experience and feedback from both the gatekeeper and third parties, whilst the Commission would expect others to be fully effective from the outset and unlikely to change thereafter.

7. ANNEX

7.1. 'Structured Dialogue' in the Telecommunications Sector

We have used telecommunications because the implementation of Articles 6(9) and 7 will have some similarity to the implementation of number portability between telecommunications operators or the implementation of interconnection arrangements, although we recognise there will also be important differences. These include the fact that such obligations are generally reciprocal in telecommunications, were implemented based on (at least some) pre-existing technical standards and involved payments between the operators concerned.

For both interconnection and number portability, it has been common for the regulated telecommunications operator to convene (or to be required by the regulator to convene) expert working groups which consist of representatives from the gatekeeper and third parties to oversee the implementation of the new regulatory requirements.[184] In telecommunications, this is normally undertaken at the national level, but in the case of the DMA, we would expect it to be undertaken on a pan-EU basis.

In its report on implementing Article 7 of the DMA, BEREC (the body of European Telecommunications Regulators) has stated:

> BEREC believes that it will be crucial to set up a structured regulatory dialogue with the interested parties (e.g., gatekeepers and providers requesting interoperability), in order to correctly define and update the reference offer. Over the past decades, telecommunication NRAs [National Regulatory Authorities] have organised, chaired or participated in structured multi-stakeholder committees or fora where concerned parties can share valuable information for the definition and update of the reference offer, and where issues and obstacles to its correct implementation can be identified and solved.[185]

[184] As BEREC noted in its opinion on the DMA proposals: 'For instance, in the electronic communications sector, national regulatory authorities (NRAs) have set up, overseen and participated in technical committees with stakeholders and/or experts to collect relevant information needed to ensure an effective and efficient design of their intervention. A typical example is the implementation of number portability, a remedy which has proven to be successful in reducing end-users' switching costs among different providers and fostering competition on the merits. In order to correctly design this remedy, NRAs gathered experts' technical inputs by organising specific fora with stakeholders (e.g., operators and equipment vendors).', BEREC 2021 p. 4, at: https://www.berec.europa.eu/sites/default/files/files/document_register_store/2021/3/BoR%20(21)%2035%20BEREC%20Opinion%20on%20the%20DMA%20-%20final.pdfhttps://www.berec.europa.eu/sites/default/files/files/document_register_store/2021/3/BoR%20(21)%2035%20BEREC%20Opinion%20on%20the%20DMA%20-%20final.pdf.

[185] BEREC Report on interoperability of NI-ICS 2023 p. 34 at : https://www.berec.europa.eu/system/files/2023-06/BoR%20%2823%29%2092%20BEREC%20Report%20on%20interoperability%20of%20NI-ICS.pdf. https://www.berec.europa.eu/system/files/2023-06/BoR%20%2823%29%2092%20BEREC%20Report%20on%20interoperability%20of%20NI-ICS.pdf

Key questions when convening such working groups include:

- Whether the groups are convened and *chaired* by the regulated firm, the regulator, or some independent party;
- The *scope of work and terms of reference* (with the intention often being, as is often the case with standards organisations such as the IETF, that technical representatives are expected to attend in a personal capacity to collectively solve technical challenges rather than seeking commercial advantage);
- Which *organisations can participate* in the working group (including whether the Commission has an observer or some other role in the group);[186]
- How disagreements or *disputes* within the working group are to be resolved, including escalation to some other oversight body or to the Commission. In the latter case, there is a delicate balance to be struck to ensure that participants do not engage in strategic behaviour or undermine trust inside the working group (e.g., to influence the regulator later in the process) but that the regulator is not excluded from being able to intervene, or participants are not prevented from appealing to the regulator when it is appropriate to do so.[187] We discuss this further below;
- How *competition law* is to be complied with whilst allowing the groups to function effectively.

Sometimes these arrangements are placed on a **more formalised** footing, as illustrated by the creation of the Office of Telecommunications Adjudicator (OTA) in the UK in 2005. The OTA describes its role as facilitating "the swift implementation of processes where necessary to enable a wider range of Communications Providers and End Users to benefit from clear and focussed improvements, in particular where multi-lateral engagement is necessary. The OTA will also be able to bring all parties together to find prompt mediated resolution of working-level implementation issues."[188] The OTA is chaired by a member of a small independent secretariat which is funded by the members and oversees, amongst other things, the implementation of number porting arrangements in the UK.

[186] In some cases, it may be that members of the High Level Group established by Article 40 might be more suitable attendees than the Commission itself. For example, BEREC might be involved in the implementation of Article 7 given the work it has already undertaken on it.

[187] Based on experience in telecommunications, conflicts can arise if the gatekeeper has limited resources to allocate and so must decide between competing requests from third parties. The gatekeeper will be expected to ensure that changes do not unduly favour its own services, but the effect of any particular change may still be to benefit some third parties over others. Sometimes requests from one third party may be strongly opposed by another. At other times some parties may argue that implementation should be delayed whilst others want it accelerated. There is no obvious solution to this, but setting out clear guidelines that explain how the gatekeeper will allocate its resources and take decisions but new functions or capabilities may assist.

[188] See http://www.offta.org.uk/.

Although working groups of this kind often focus on **technical issues**, including technical standards, **other non-technical ad hoc groups** may need to be convened to address operational or legal matters. This can include:

- The development of ***a standard contract*** for the provision of the service (referred to as the Reference Offer in Article 7 of the DMA and clearly modelled on the Reference Offers that are required to be produced by the European Electronic Communications Code (EEEC)).[189] This will include standard commercial terms, such as indemnities, IP rights, termination clauses, NDAs etc. We think **reference offers** (whether they called that or not) will also likely be required – as a practical matter - to effectively implement Articles 6(9), (10), and (11) even though this is not expressly envisaged by the DMA;[190]

- ***Ordering and validation processes*** to ensure that the service required is the one being delivered (e.g., in relation to Articles 6(9), (10), and (11) different third parties may have differing data requirements and the gatekeeper may need or wish to offer a limited menu of options rather than bespoke arrangements to meet each request). This aspect may be particularly important if the gatekeepers require third parties to 'pre-qualify' in some way in order to ensure that security, privacy or integrity concerns are addressed;[191]

- The definition of ***service levels*** (e.g., target availability of connections or APIs), service guarantees and key performance indicators (KPI). These may be particularly important when wholesale services are to be provided without charge, since non-price discrimination (or simply poor quality) is then the main risk to effective implementation.

- ***Fault reporting arrangements*** **and escalation processes**. These are important in telecommunications, as it was often unclear whether responsibility for a failure (e.g., to process customer consent to port data) lay with the third party (incorrect submission of the form etc.) or

[189] Article 69(2) of the EECC allows regulators to require undertakings to publish reference offers whilst 69(3) allows the regulator to impose changes to the reference offer. The latter normally involves requiring amendments to specific provisions to better ensure compliance with obligations rather than the regulator replacing the reference offer produced by the regulated firm with one of its own. The DMA does not address this directly, but we assume the specification process envisaged by Article 8 would allow the Commission to require specific changes to a reference offer. The publication of a reference offer is justified in telecoms on the grounds that it ensures transparency in conditions of supply and guards against discrimination (since all third parties sign the same contract). In practice, reference offers also greatly facilitate the effective and rapid implementation of obligations and avoid duplication and conflict.

[190] We suspect the reason they are not referred to may be that BEREC was less involved in advising the Commission on Article 6 than Article 7.

[191] In other data sharing arrangements, such as Open Banking in the UK, for example, those requesting data must be registered with the regulator and fulfil certain conditions of registration. This does not appear to be anticipated by the obligations in the DMA, although refusals to supply a particular third party would presumably be referred to the Commission or a national authority.

the regulated firm (failure to process a form that was correctly submitted). The same may apply with the DMA.

- ***Testing arrangements*** to be completed by the regulated firm and third party prior to the activation of the service.
- ***Forecasting requirements*** to ensure adequate provisioning of capacity by the regulated firm (including provisions if forecasts subsequently prove inaccurate).

We noted in the introduction that measures to ensure compliance with the DMA are likely to evolve over time (whilst recognising that the assessment of effectiveness and hence compliance will be undertaken by the Commission on the basis of the information available to it at a particular point in time). Experience from telecommunications suggests that gatekeepers or third parties may propose **changes to the way in which obligations are implemented in light of the experience of their implementation**. These changes may be mutually beneficial for both the third party and the gatekeeper but are likely to require an agreed process for the receipt and assessment of 'change requests' that are made to or by the gatekeeper. Similarly, it is conceivable that third parties may submit requests to the gatekeeper for additional wholesale services which are not required or currently required by regulation but that the gatekeeper considers it would nonetheless be in their commercial interests to supply. Although this may be unlikely in the short term for the DMA, experience from telecommunications (and Open Banking) suggests that regulated firms often start by supplying the minimum required for compliance but that, over time, other commercial opportunities will be identified alongside those regulatory requirements.[192] Experience also suggests that market participants may be better placed to update the scope and implementation of regulatory obligations than the regulators themselves.

This suggests that the processes and forums that are created to implement the obligations of the DMA are required to allow both the gatekeeper and third parties to oversee the ongoing operation of the arrangements that have been put in place and to develop them further. The intensity and nature of the work may change, but **some structured form of ongoing interaction between the regulated firm and the third parties it supplies is likely to be required for at least some obligations.** A responsive gatekeeper should wait for findings of non-compliance before engaging in such a dialogue.

[192] For example, the Open Banking Implementation Entity in the UK first developed a series of 'regulated products' but is now expected to provide a forum for the development of other services on a purely commercial basis, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf.

cerre Centre on Regulation in Europe

DMA OUTPUT INDICATORS

RICHARD FEASEY
ALEXANDRE DE STREEL

1. DMA COMPLIANCE REPORTS

The aim of the **obligations introduced by the Digital Markets Acts (DMA)** and imposed on gatekeepers is to influence the conduct of gatekeepers and, by so doing, to advance the overall objectives of **contestability and fairness** in digital markets.[193] The impact on competition and market outcomes will, however, also depend upon how and whether users or other firms take advantage of the new opportunities that the obligations are intended to create by facilitating entry by firms and allowing users to exercise choices that have not previously been available to them. **How and the extent to which users and firms do this will be determined by whether the gatekeeper complies with its obligations but also by many other factors outside of the gatekeeper's control**.

The impact of obligations might also be expected to **change over time**, with more limited effects being seen when the DMA is first implemented and more significant effects being seen later as other firms and users take time to respond to the opportunities that arise.

The European Commission is responsible for enforcing the DMA and ensuring that gatekeepers comply with their obligations under Articles 5, 6, and 7. Article 8 requires the gatekeeper to produce a **compliance report** within 6 months after the designation that describes "the measures it has implemented to ensure compliance".[194] These reports are then required to be updated on an annual basis. Article 8 does not specify the evidence or information which a gatekeeper is expected to provide to the Commission but it appears to envisage a description of the 'process measures' that have been implemented by the gatekeeper. Article 26 also requires the Commission to "take the necessary actions to monitor the effective implementation and compliance with the obligations laid down in Articles 5, 6, and 7" without specifying what those actions might be.

The Commission is consulting on what it calls a standard **'template' for compliance reports**, including the contents of those reports.[195] The Commission currently envisages this to be a mixture of '**process measures**' which explain the actions the gatekeeper has taken in order to comply but also:[196]

"a **set of indicators** which allow – or will allow based on their future evolution – to assess whether the measures implemented by the gatekeeper to ensure compliance are 'effective in achieving the objectives of the DMA and of the relevant obligation', as required by Article 8 DMA, including an explanation why the gatekeeper think that these indicators are the most relevant;

any relevant **data** which can inform whether the measure is or will be **effective** in achieving the objectives of the DMA, such as, depending on the circumstances, data on the evolution of the number

[193] Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1.

[194] On the key importance of those compliance reports, see J. Cremer, D. Dinielli, P. Heidhues, G. Kimmelman, G. Monti, R. Podszun, M. Schnitzer, F. Scott-Morton, A. de Streel, Enforcing the Digital Markets Act: Institutional Choices, Compliance, and Antitrust, *Journal of Antitrust Enforcement*, 2023

[195] Template for reporting pursuant Article 11 DMA: https://ec.europa.eu/eusurvey/files/7635871b-5946-4a39-b9b7-3491143f3128/a61347f2-d113-42db-a5a4-33df0fe49c28

[196] Section 2.1.2 of the template, points k, r and s (our emphasis).

of active end users and active business users for the relevant core platform service and, for each relevant obligation, data on the evolution of the fees and revenue share for the relevant services, the interaction of end users with choice screens and consent forms, the amount of in-app purchases, the amount of pre-installed defaults, counts of end users who switch, counts of business users who obtain data access, etc.; and any **internal systems and tools** used to monitor the effectiveness of the measure and the output of such internal systems and tools".

This **paper recommends that the Commission should also require gatekeepers to report against a common set of 'output indicators'**. These might be in addition to some of the data referred to above, or might substitute for some of it. In the rest of this paper, we first explain what 'output indicators' are, and how they are situated in relation to other types of indicators or other evidence relevant to an assessment of compliance. We then make recommendations as to how they should be implemented. A proposed list of suitable indicators in relation to Articles 5, 6, and 7 will be published later in 2023, separately.

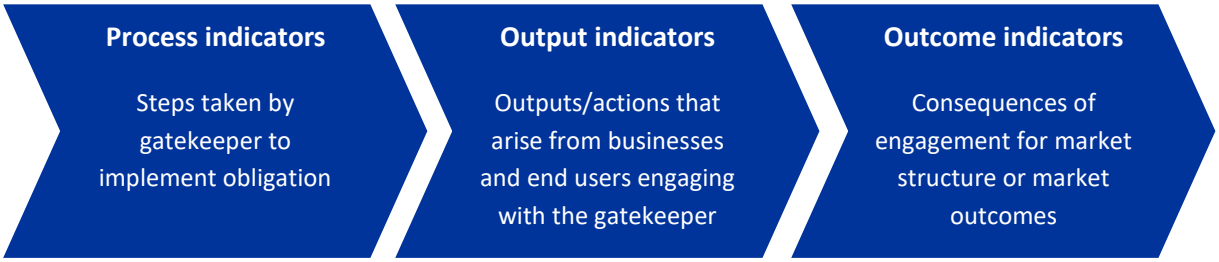
Article 21 of the DMA provides the Commission with powers to require any information from undertakings to enable the Commission to discharge its duties. The proposals in this paper envisage that data relating to the output indicators we propose would be requested from gatekeepers and be published by them.

2. DEFINITION AND FUNCTION OF OUTPUT INDICATORS

2.1. Definitions

Output indicators should provide the Commission with evidence, **alongside other information** submitted by the gatekeeper, third parties, or assembled by the Commission itself, **that inform an overall assessment of whether the gatekeeper has complied** with the relevant obligation (as well as potentially allowing the Commission and the gatekeeper to diagnose why non-compliance has occurred and what steps might be required to remedy any breach).

One approach to **assessing compliance is by reference to the processes** that are adopted by the gatekeeper to comply with the rules, on the assumption that these processes will thereby influence the gatekeeper's conduct and market outcomes. Another view is that **compliance should be assessed by reference to the actual outcomes** or changes in competitive conditions or market structures which result from the gatekeeper's conduct, with the means by which they are achieved being left unexamined and for the gatekeeper to determine. These approaches are not mutually exclusive. The **output indicators** that we propose can be thought of as being **situated downstream of process indicators but upstream of outcome indicators**:



Output indicators are intended to capture both the extent to which conduct by the gatekeeper has created new opportunities for firms or users *and also* the extent to which firms or users have engaged with those opportunities with respect to a particular gatekeeper. In contrast, **outcome indicators** will measure how market outcomes as a whole are affected by these outputs, such as how prices or market shares change in response to action being taken by one or a number of gatekeepers within a particular market or as a result of other factors that may be unrelated to the actions of gatekeepers or their compliance with the DMA.

2.2. Functions

Views also differ about whether compliance can or should be **assessed against particular targets** that are specified in advance or whether the focus should be on the **direction** of travel rather than any specific threshold. The output indicators we propose are not targets. They are intended to help the Commission (and gatekeepers and third parties) understand **what is happening in a dynamic sense rather than to establish whether a gatekeeper can be said to have complied with its obligations or to have achieved a particular target**. Output indicators are intended to provide information about the impact of changes in the gatekeeper's conduct, particularly over time, and the overall direction of travel rather than a 'snapshot' assessment.

An important feature of output indicators is that, provided the methodologies and metrics are specified in advance and remain **consistent through time**, they will allow the Commission (and gatekeepers and third parties) to understand how the effects of various measures being taken by the gatekeeper are changing over time.

They are also intended to **allow for comparison or benchmarking between gatekeepers** providing the same Core Platform Service, albeit this should only provide a basis for further investigation of differences in outputs rather than allowing for any immediate conclusions about compliance to be drawn from such a comparison. We also recognise that comparisons concerning some CPS and some obligations may be less appropriate and more challenging than others. This may be the case with respect to 'online intermediation services' where the business model adopted, market conditions faced or end or business users served by one gatekeeper may be quite different from those of another. This could mean, for example, outputs indicators with respect to Article 6(9) DMA (i.e., porting of data) may be quite different for a gatekeeper providing a service in a market in which multi-homing is commonplace from a gatekeeper providing a service in a different market in which it is not. We, therefore, recognise that comparison for some CPS may not be appropriate or possible either because the gatekeepers providing the CPS operate in different markets and serve different users or because only a single gatekeeper has been designated in respect of that CPS. On the other hand, comparison will be useful when several gatekeepers provide the CPS under similar market conditions and to the same groups of business and end users.

Comparison is more difficult with respect to process measures, which may differ significantly between gatekeepers, or if different gatekeepers are left to propose or adopt their own indicators (as the Commission's draft standard template for compliance reports currently seems to envisage). **Outcome measures** will capture the aggregate effect of the implementation of measures by all gatekeepers on the market, but it may be impossible to attribute these outcomes to actions taken by any individual gatekeeper. Output indicators avoid both of these challenges.

2.3. Limits

However, it is important to note that **output indicators have some shortcomings**. First, output indicators may provide a measure of the consequences of a user's interaction with the gatekeeper (in terms of switching or providing consent) but they do **not offer any assessment of the users' experience** when doing so (in terms of whether they understood the choices presented to them or the basis on which they made their decision or did not act). Process indicators may assist here, but other investigative tools may also be required. Process indicators may be required to assess the extent to which compliance is or is not inhibited by the gatekeeper taking measures that it justifies as being needed to ensure the **integrity of hardware or operating system or security** in relation to third-party party apps or app stores, as provided for in Articles 6(4) or 6(7).

Second, some output indicators may refer to aggregate outputs or averages, which may **disguise important underlying variances**. For example, Article 6(5) relates to organic search result rankings

across all search categories but this may disguise significant variances in outputs between these categories[197].

Third, in common with outcome indicators, output indicators **may be influenced by factors other than the conduct of the gatekeeper** or their compliance with the DMA obligations. However, unlike outcome indicators, these factors are likely to be common to all gatekeepers with respect to the indicator in question, meaning that comparison between them may still pick up differences that are attributable to the conduct of the gatekeeper itself rather than these other factors. Gatekeepers will obviously have an opportunity to explain the factors which may account for such differences (e.g. over time or between gatekeepers in the same time period).

Therefore, European **Commission will need to use the output indicators, alongside other evidence**, to decide whether the steps which the gatekeeper has taken and the outputs which result mean that the gatekeeper is or is not complying with its obligations at any particular point in time. Output indicators are intended to perform a complementary (but important) role in the Commission's compliance assessment alongside other evidence that it may collect or that the gatekeeper or others may submit.[198]

We recommend that the Commission give further consideration as to what **other evidence is required to complement the output indicators** and the gatekeeper compliance reports. This could include the use of **surveys or A/B testing** to allow the Commission (and others) to better interpret indicators. For example, output indicators that suggest that end users have been unable to benefit from the choices which the DMA obligations are intended to confer will need to be interpreted by reference to other evidence on whether end users were able to exercise a choice but chose not to do so whilst indicators which suggest that end users have been able to and have exercised a choice may not reveal how well informed they were when doing so. If survey or A/B testing evidence is to be used in this context, then we recommend that the gatekeeper is required to consult with the Commission before the survey or testing is undertaken and that the **Commission first approve the methodology** and approach. This does not preclude gatekeepers from submitting other surveys or testing evidence that they consider relevant to the Commission's assessment of compliance, and we would expect them to do this.

[197] In the absence of industry-agreed categories for search queries (e.g. travel, shopping) we do not propose further indicators for Art 6(5) at this stage but such data may be submitted by gatekeepers as part of the compliance report.

[198] One important issue that has arisen during this project is whether output or outcome indicators are required to assess the extent to which the DMA obligations lead to users replacing a service provided by the gatekeeper with a service provided by another service provider (i.e. single-homing) or whether implementation leads to use of multiple services (i.e. multi-homing). This may have important implications for the way in which competition might develop but it is not something directly relevant to the compliance assessment which the Commission is required to undertake.

3. SPECIFICATION AND IMPLEMENTATION OF THE OUTPUT INDICATORS

3.1. Specifications

Quantitative measurement for the purposes of assessing compliance cannot of course start until gatekeepers have taken steps to comply with their obligations[199]. However, we recommend that the **indicators be specified by the Commission in advance of the implementation of the DMA** (which would differ from the template for the compliance report itself, on which the Commission is currently consulting) rather than, for example, waiting until the first compliance reports are produced or data is published. This may allow gatekeepers to take their output indicator reporting obligations into account when designing the processes to ensure compliance and, perhaps more importantly, it will provide a baseline reading prior to implementation against which subsequent measurements can then be compared.

It would be desirable if the **initial set of output indicators were to be adopted following a process that involves participation by all stakeholders**, as this CERRE project has sought to do. This is particularly important because some of the data which we envisage gatekeepers would collect and publish using output indicators as a benchmark may not be collected by some gatekeepers in the ordinary course of business, although we expect that much of it would. During the consultation with the Commission, it will be open to gatekeepers to make representations to the Commission as to any additional costs they expect to incur in producing particular indicators and the practicality of doing so. We also recognise that the consultation of the Commission will not avoid disputes about how a particular set of measurements should be interpreted later, what conclusions should be drawn from them, or how much weight should be attached to them relative to other evidence.

It should also be noted that for a number of obligations, we consider that no appropriate quantitative indicator exists, or that outputs are better assessed using other evidence. Output indicators are intended to be informative about a relevant aspect of the obligation in question and to contribute to an assessment of compliance, as well as being capable of being produced by the gatekeeper based on data that we expect it to collect and to hold. The **list is not intended to be exhaustive and may need to be revised in light of experience** of their application or as changes are made to obligations, although it is also important that indicators remain consistent and relatively stable over time and are not subject to regular change.

In order to enable comparability and ensure early implementation, we recommend that **gatekeepers are required to adopt the same output indicator for each obligation** under Articles 5, 6, and 7. This

[199] This raises a question of when the relevant time period should start from, since some gatekeepers may begin to implement their obligations, and the effects may be observed, in advance of the deadlines set by the DMA. Our recommendation is that gatekeepers should be expected to collect data for indicators in the month *before* they take steps to comply so as to provide a baseline measure against which subsequent measures can be compared. We are also aware that some outputs may be subject to seasonal variation and would expect gatekeepers to indicate this, if relevant, when publishing the data.

may require the European Commission to issue a decision under Article 21 which specifies the indicators against which the gatekeeper, or gatekeepers in general, is required to report.

It is also important that the **data is sufficiently disaggregated** to be informative and to allow third parties to understand whether their own experience may differ from that of the market as a whole.

At the same time information that is published should **not reveal commercially sensitive information to the material detriment of either the gatekeeper or any third party**. In particular, a question arises as to whether requiring gatekeepers to report against certain output indicators[200] would require them to have access to information about the functioning of third-party applications and services which they would otherwise not be expected to have access to in the normal course of business and which may be of commercial value. It would not be desirable if a requirement to produce output indicators to assess compliance were to lead to the gatekeeper obtaining access to such information. We recommend the Commission assess each indicator to ensure that its production does not require disclosure of commercially sensitive information to the gatekeeper which would not otherwise occur.

3.2. Implementation

The Commission will also need to consider how frequently output indicators should be produced and published. One of the motivations for the DMA is that existing approaches have been too slow in assessing and remedying issues that arise in fast moving digital markets. This points in favour of more frequent publication. Once the gatekeeper has implemented measures to collect and report the relevant data, we do not think that requiring regular reporting and publication of the output indicators will impose any significant additional costs upon the gatekeeper. We, therefore, recommend that **gatekeepers be required to report against output indicators on a quarterly basis**. We consider that quarterly output indicators would provide the European Commission with useful insight into the effects of the implementation of the DMA obligations in the intervening period between annual compliance reports.

We further recommend that the quarterly output indicator reports be **reviewed and approved prior to publication by the Compliance Officer of the gatekeeper** as part of their function under Article 28(5) (as the Commission envisages for the annual compliance report). The quarterly report should explain the methodology adopted by the gatekeeper in its production and highlight any changes in methodology from the previous relevant period.

In circumstances where the Commission has reasonable grounds for thinking that the gatekeeper had failed to produce an output indicator in the manner specified by the Commission (e.g. has interpreted the measure in a different or more favourable way without seeking guidance from the Commission) then the Commission should consider requiring an **independent audit** of the output indicator report before it is supplied to the Commission, exercising its powers under Article 26(2) to do so.

We recommend:

[200] For instance, Art 6(4) indicator relating to third party apps downloaded from a third-party app store.

- Output indicators are reported by the gatekeeper to the Commission on a country by country basis[201] but published on an aggregated EU-wide basis;
- Output indicators that refer to third-party apps are reported by the gatekeeper to the **Commission on a disaggregated basis** (i.e. by reference to each third-party app provider subject to some de minimum threshold) but the data is published on an aggregated ('all third-party apps') basis.
- Each **third-party provider receives the output indicator data applicable to its own services** from the gatekeeper (on a confidential basis) at the same time as the aggregated data is published.
- We have also considered carefully where whether output indicators should be disaggregated by reference to the platform over which the CPS is consumed (e.g. smartphone vs PC vs digital assistant). Whilst there may be legitimate reasons (e.g. security or other technical considerations) for the implementation of the obligations to differ between, for example, the smartphone and PC environment, we have concluded that it would be useful to compare output indicators relating to the same CPS and gatekeeper and obligation, as applied on different platforms. We, therefore, recommend that output indicators are reported by the gatekeeper to the Commission on a **platform-specific basis** (smartphone, PC, TV, and so on) and that they are published by the gatekeeper on this basis.

[201] We recognise there may be some issues with end users who interact with the gatekeeper whilst roaming, but do not consider these are likely to have a material effect on the results however treated in the report

Explanatory Notes

Below is an illustrative list of output indicators that might be adopted by gatekeepers or requested by the European Commission. The current version of the European Commission's Compliance Report Template for gatekeepers does not require gatekeepers to adopt output indicators nor specify which indicators might be appropriate. The list below is extensive, with some Articles having many more indicators than others (and some having none at all). We expect that only a sub-set of indicators would be adopted, at least initially, particularly if a common set of indicators for all gatekeepers were to be specified by the European Commission. We also expect that the list could be modified over time as some indicators become less relevant or otherwise prove inappropriate.

The purpose and function of output indicators is further discussed in the accompanying CERRE paper on Output Indicators: they are intended to inform the assessment of compliance, which we expect to also rely upon other qualitative data. We would expect gatekeepers to wish to comment on figures that are produced (as part of the Compliance Report) in order to inform how they might be interpreted and what weight might be attached to each. Third parties in receipt of a non-confidential version of the Compliance Report may also wish to comment and we assume that output indicators would generally be presumed not be confidential in this context.

Some indicators in the list below measure flow or the rate of change from one period to another and some measure stocks or the cumulative impact of the measures to date. As explained further in the accompanying paper, output indicators are intended to allow the Commission (and others) to observe changes in the effect of measures taken by the gatekeeper as third parties, including end users, engage with them over time. Some indicators are intended to aid understanding of how and why end users or third parties may or may not be engaging with measures, although other sources of evidence, such as surveys, may also be helpful in this regard.

Most indicators would be expressed (and published) as a percentage in order to enable comparison of the common indicators between gatekeepers, which we consider an important feature of our proposal and which is discussed further in the accompanying paper. However, care will be required when interpreting percentage figures that are based on low sample sizes or for which the sample size is changing significantly from one period to the next (although in the majority of cases we expect the samples to be both very large and relatively stable over time). Gatekeepers would be expected to supply the underlying data from which the percentages are derived to the European Commission, but not to publish it. Some indicators measure the volume of output (e.g. % of advertising spend or % of apps downloaded etc) and some measure the proportion of users (e.g. % of users) without distinguishing between the significance of different users. The impact of a provision on competition will of course depend both on the number of users taking advantage of the opportunity provided by a measure and the relative economic significance of those which do.

DMA Obligation	Quantitative output indicator	Commentary
Art 5(2): use of personal data acquired from CPS without consent and sign into other services	A. % of active end users (as % of total end users at the end of the relevant period) from whom consent was sought by the gatekeeper for the processing, combination or cross-use of personal data during the relevant period	The aim of this provision is to prevent gatekeepers from using personal data for other services without end user consent. Indicator A is a 'flow' measure of the extent to which gatekeeper has actively solicited consent for processing, combining or cross-using data (as opposed to not using personal data in this way or doing so without consent). This will likely be influenced by (a) the extent to which the gatekeeper wishes to process, combine or cross- use data (b) the number of consents already obtained in prior periods (c) the number of new end users acquired in the relevant period (d) the number of consents previously withdrawn or withheld. The measure allows for assessment of gatekeeper activity over time (i.e. across different relevant periods). It could be further broken down into separate consents for each activity depending on how implemented by gatekeeper or interpretation of 'specific choice'.
	B. % of active end users (as % of end users at the end of the relevant period) for whom the gatekeeper has obtained consents for the processing, combination or cross-use of personal data at end of relevant reporting period	This is a 'stock' measure of the cumulative level of user consent obtained by gatekeeper and provides an indication of the impact of the consent requirement in enabling or inhibiting the gatekeeper's use of personal data. Comparison may suggest some gatekeepers have processes that are more effective at obtaining consents that others or that some are more reliant upon leveraging personal data than others.
	C. Of those active users from whom consent for the processing, combination or cross-use of personal data was sought during the relevant period (a) % of these actively declining to consent during the same period (b) % declining to make a choice when asked to do so	This measure allows for more detailed assessment of user responses to the provision (A measures gatekeeper conduct, C measures user response). It breaks down non-consents into users actively rejecting request and those simply not responding. It may allow assessment of effectiveness of consenting process and fatigue over time.
Art 5(3): no MFNs	N/a	The aim of this provision is to remove restrictions in contracts between the gatekeeper and business users which inhibit the ability of the latter to offer favourable terms through rival sales channels. Compliance would be assessed by reference to process measures governing contracts or on a case by case basis rather than by means of output indicators.

Art 5 (4 & 5): services consumed via CPS if not purchased through them	A. % of active end users (as a % of all users of all third party services or as a % of all users) that used third party services on the CPS during the relevant period for which they did not contract, register or otherwise subscribe to through the CPS in the relevant period or any prior period B. Number of active end users that used third party services on the CPS during the relevant period for which they did not contract, register or otherwise subscribe to through the CPS in the relevant period or any prior period	The aim of these provisions is to allow business users and end users of the CPS to interact with each other outside of the CPS as well as on the platform. This includes business users making offers to end users as well as end users consuming services on the CPS that have been contracted for outside of it. The indicator does not directly measure the ability of business users to make offers for services outside the CPS or the effectiveness of such offers but instead measures the ability of end users to then consume services over the CPS for which they contracted elsewhere. Individual suppliers of third party services may be able to produce this indicator for their own services, but not in aggregate for the CPS as a whole. The measure allows for assessment of changes over time and for comparison between gatekeepers at a particular point in time. Indicator B is similar to A, but expressed in terms of absolute number of users rather than proportion of the user base The indicators could be further broken down by service category, likely to be defined by the gatekeeper, to better understand the impact of the provision on different categories of service.
Art 5(6): do not inhibit complaints	N/a	The aim of this provision is to prevent the gatekeeper restricting the ability of business users to bring complaints about non-compliance to the EC or other regulators. This would be revealed if business users were nonetheless to reveal that they were subject to such restrictions. No suitable for output indicators and likely to be assessed on a case by case basis.
Art 5(7): no tying of ID, browser engine or payment service with CPS	A. % of active end users (as % of total end users at the end of the relevant period) that used an ID service provided by the gatekeeper during the relevant period	The aim of this provision is to prevent the tying of other gatekeeper services to the CPS and so allow end and business users to use non-gatekeeper ID, web browser or payment services in conjunction with the CPS. Indicator A measures the extent to which business users (and by implication end user customers of those business users) used gatekeeper ID services in a given period, providing a crude indication of the extent to which business users may also be using non-gatekeeper ID services as the provisions are intended to allow them to do. It does not allow identification of those business users who did not use any ID services in the period or those which may use both gatekeeper and non-gatekeeper ID services in the same period.

	B.% of active end users (as % of total end users at the end of the relevant period) that do not use ID services provided by the gatekeeper during the relevant period but did in the previous period	This is an indicator of the proportion of business users that have switched and, by implication, the ease with which business users can switch from a gatekeeper to non-gatekeeper service between two relevant periods. It does not allow identification of those business users who decide not use any ID service or those which retain the gatekeeper ID service but do not use it in the relevant period. It is a crude measure of the contestability of ID services
	C. % of active end users (as % of total end users at the end of the relevant period) that used a web browser engine provided by the gatekeeper during the relevant period D. % of active end users (*as* % of total end users at the end of the relevant period) that do not use a web browser engine provided by the gatekeeper during the relevant period but did in the previous period E. % of active end users (as % of total end users at the end of the relevant period) that used a payment service provided by the gatekeeper during the relevant period F. % of active end *users (as* % of total end users at the end of the relevant period) that do not use a payment service provided by the gatekeeper during the relevant period but did in the previous period G. % of active end users (as % of total end users at the end of the relevant period) that used technical services that support the provision of payment services provided by the gatekeeper during the relevant period H. % of active end users (as % of total end users at the end of the relevant period) that do not use technical services that support the provision of payment services provided by the gatekeeper during the relevant period but did in the previous period.	This (and those that follow) are the same indicator as for ID services above but applied to web browsers, payment services and technical services that support the provision of payment services. They will provide an indication of both the ability of rivals to offer competing services (which is relevant to the compliance assessment) and of the willingness and ability of end users to switch to them (which may not be relevant). Further investigation of the factors behind the figures would be required if concerns about compliance were to arise in this context.

Art 5(8): no unfair bundling of CPS	A. % of active end users (as % of end users registering for the CPS in the relevant period) that have rejected a request to subscribe to or register with a further CPS provided by the gatekeeper during the relevant period	The aim of this provision is to prevent the tying of a particular CPS with other CPS provided by the same gatekeeper. Indicator A measures the extent to which users have registered for the gatekeeper CPS in the relevant period without choosing to take other CPS from the gatekeeper at that point. The ability of users to decline to register for other CPS whilst registering for CPS is an indicator of absence of tying. Allows for assessment of user responses over time and impact of changes to the registration process.
	B. % of business users (as % of business users registering for the CPS in the relevant period) that have rejected a request to subscribe to or register with a further CPS provided by the gatekeeper during the relevant period	This is the same measure as A but applied to business users.
Art 5(9): data for advertisers	A. % of total advertising spend attributed to advertisers (or third parties) in the relevant period who have been provided with information on daily fees and other charges during the relevant period (for each of the relevant online advertising services provided by the gatekeeper on the CPS	The aim of the provision is to allow advertisers to obtain granular information about advertising costs from the gatekeeper. Indicator A measures the impact of advertiser/third party requests for data which does not require publisher consent to divulge by reference to the share of spend/gatekeeper revenue attributed to those requests. It also measures the extent to which advertisers respond to the opportunity to request such information and the potential usefulness and impact of the measure. It allows for assessment of advertiser behaviour over time and comparison between different advertising services offered by the gatekeeper.
	B. % of total advertising spend attributed to advertisers (or third parties) in the relevant period who have been provided with information on publisher remuneration during the relevant period for each of the relevant online advertising services on the CPS	Indicator B is similar to A but applies to requests for publisher remuneration information which does require publisher consent.
	C. % of total advertising spend attributed to advertisers (or third parties) in the relevant period for which publisher remuneration information has been withheld by the gatekeeper due to publisher non-consent for each of the relevant online advertising services provided by the gatekeeper on the CPS	Indicator C is a measure of the extent to which the provision of information by gatekeepers to advertisers is inhibited by a refusal of publishers to give consent to share remuneration data. Comparison may show differences in consent mechanisms amongst gatekeepers or the impact of changes over time.

	D. % of publishers (as % of total publishers served by the gatekeeper in the relevant period) that withheld consent to the sharing of information regarding the remuneration received during the relevant period or each of the relevant online advertising services provided by the gatekeeper on the CPS	Indicator D is similar to C but is a measure of how requests for consent are received by publishers in general, without regard to differences in their size/revenue. Comparison may show the impact of changes to consent mechanism or publisher attitude to such requests.
Art 5(10): data for publishers	A. % of total publisher remuneration attributed to publishers (or third parties) who have been provided with information on daily remuneration received and fees paid during the relevant period for each of the relevant online advertising services provided by the gatekeeper on the CPS B. % of total publisher remuneration attributed to publishers (or third parties) who have been provided with information on prices paid by advertisers during the relevant period for each of the relevant online advertising services on the CPS C. % of total publisher remuneration attributed to publishers (or third parties) for which advertiser price information has been withheld by the gatekeeper due to advertiser non-consent for each of the relevant online advertising services provided by the gatekeeper on the CPS D. % of advertisers that withheld consent to the sharing of information regarding advertising prices paid during the relevant period or each of the relevant online advertising services provided by the gatekeeper on the CPS	These indicators are similar to those for 5(9), but apply to information provided by the gatekeeper to publishers, including information (prices paid) for which consents from advertisers is required.
Art 6(2): not to use third party business user	N/a	This provision prohibits the gatekeeper using data generated by business users or their customers over the CPS to compete with those same business users. This is not susceptible to

data acquired via CPS		measurement by an output indicator and compliance would likely be demonstrated by process measures (and non-compliance by complaints on a case by case basis)
Art 6(3) Allow uninstallation of apps		The aim of this provision is to enable end users to easily uninstall gatekeeper apps and to easily apply default settings for third party (as well gatekeeper) apps.
	A. % of gatekeeper apps (as % of total installed gatekeeper apps at the end of the prior relevant period) that have been uninstalled during the relevant period for each gatekeeper app and each type of OS	Indicator A is a flow measure of the proportion of gatekeeper apps that are uninstalled in the relevant period and, by implication the ease and willingness of users to uninstall gatekeeper apps. It allows assessment of changes over time and comparison between different apps and types of OS.
	B. % of active end users that uninstalled a gatekeeper app, for each gatekeeper app, during the relevant period	Indicator B is a measure of the propensity of users to uninstall gatekeeper apps, whereas A measures the extent to which uninstallation is taking place in aggregate. Indicator B may be a better indication of the impact of changes in choice architecture on the uninstallation process.
	C. % of active end users (as a % of total end users at the end of the relevant period) that initiated uninstallation process for a gatekeeper app (excluding software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third parties) but did not complete uninstallation in the relevant period	Indicator C is intended to be a measure of the ease with which uninstallation is achieved and therefore any obstacles which may inhibit uninstallation process for gatekeeper apps by reference to attempts to uninstall apps which do not complete. A similar measure is proposed for Art 6(4)
	D. % of active end users (as a % of total end users at the end of the relevant period) that uninstalled and then reinstalled a gatekeeper app or apps in the relevant period	Indicator D measures the proportion of users who complete the uninstallation of the gatekeeper apps but then reinstall them at a later point in time within the same period. This provides further evidence as to the impact of the measure on contestability.
	E. % of active end users (as % of a total users at the end of the relevant period) that were presented with the choice box for each combination of OS and (a) search engine (b) web browser (c) virtual assistant during the relevant period	Indicator E measures the frequency of presentation of choice box by the gatekeeper. Indicators I and J decompose this measure further to isolate presentation when the device is set up or a service used for the first time. To the extent that end users are presented with the choice box on

Default settings for search engine, VA or web browser		other occasions, the gatekeeper should explain when those are and provide similar indicators as for I and J
	F. % of active end users (as a % of total users at the end of the relevant period) that were presented with the choice box when setting up a new device for each combination of OS and (a) search engine (b) web browser (c) virtual assistant during the relevant period	Indicator F allows assessment of when users are being presented with the choice box by isolating presentation at the point the user is setting up a new device
	G. % of active end users (as a % of total users at the end of the relevant period) that were presented with the choice box when first using the service for each combination of OS and (a) search engine (b) web browser (c) virtual assistant during the relevant period	Indicator G allows assessment of when users are being presented with the choice box by isolating presentation at the point the user is first using the service in question
	H. % of active end users (as % of those presented with the choice box in the relevant period) that have set the gatekeeper's service as default via the choice box for each combination of OS and (a) search engine (b) web browser (c) virtual assistant during the same relevant period	Indicator H is a flow measure of the proportion of users choosing gatekeeper's service as a default when presented with a choice in a given period. It allows assessment of the impact of changes in the choice box, frequency of presentation of choice screen and/or changes in user responses over time.
	I. % of active end users that have set the gatekeeper's service as default via the choice box in the relevant period for whom the same gatekeeper service was the default at the beginning of the same relevant period, for each combination of OS and (a) search engine (b) web browser (c) virtual assistant	Indicator I is a flow measure of the proportion of the users choosing the gatekeepers service as a default when presented with the choice box who had been using the same service as a default prior to being presented with the choice box. It is a measure of the extent to which the choice box leads users to change their consumption habits.
	J. % of active end users (as a % of all end users at the end of the relevant period) that have set the gatekeeper's service as default for each combination of OS and (a) search engine (b) web browser (c) virtual assistant at end of the relevant period	Indicator J is a stock measure of the cumulative impact of allowing users to choose their default settings, including the impact of the choice box on default settings.
	K. % of active end users (as a % of those presented with the choice box in the relevant period) that have set a third party's	Indicator K is a flow measure of proportion of users choosing third party services as default when presented with a choice. It allows for comparison with indicator H.

	service as default for each combination of OS and (a) search engine (b) web browser (c) virtual assistant as a default during the relevant period	
	L. % of active end users *(*as a % of total users at the end of the relevant period) that have set a third party's service as default for each combination of OS and (a) search engine (b) web browser (c) virtual assistant at end of the relevant period	Indicator L is a stock measure of the cumulative impact of the choice box for third party defaults.
	M. % of active end users (as % of total users at the end of the relevant period) who have changed the default setting from a gatekeeper's service to a third party service for each combination of OS and (a) search engine (b) web browser or (c) virtual assistant to a third-party service during the relevant period	Indicator M is a measure of the ease of switching defaults from gatekeeper to third party whether in response to presentation of a choice box or not.
	N. % of active end users (as % of total users at the end of the relevant period) who have changed the default setting from a third party service to the gatekeeper's service for each combination of OS and (a) search engine (b) web browser (c) virtual assistant during the relevant period	Indicator N is similar to M but a measure of switching in the opposite direction.
Art 6(4): third party applications and app stores		The aim of this provision is to enable end users to download third party app stores and to sideload third party apps if they wish, and to set third party apps or app stores as their default if they wish.
	A. % of active end users (as % of total users at the end of the relevant period) who have downloaded a third-party app store during the relevant period for each type of OS	Indicator A is a flow measure of user's response to opportunity to download third party app stores from gatekeeper store. It allows for assessment over time. Comparison between gatekeepers may allow analysis of how integrity and/or security issues are addressed by different gatekeepers.
	B. % of active end users (as a % of total users at the end of the relevant period) who initiated a download of a third party app	Indicator B is a measure of the ease of downloading third party app stores and any obstacles which may cause users to abandon the download process once commenced. It allows for assessment of the impact of changes to the download process over time.

	store in the relevant period but did not complete the download for each type of OS	
	C. % of active users who initiated but did not complete a download of a third party app store from the gatekeeper's app store in the relevant period who received (a) one gatekeeper message (b) two or more gatekeeper messages during the download process	Indicator C is a measure of the impact of messages presented by the gatekeeper to end users during the download process on end user propensity to complete the downloading of third party app stores. It does not imply any assessment of whether such messages, which may contain 'warnings' or other information scripted by the gatekeeper (rather than the third party), are justified or not.
	D. % of active end users (as a % of total users at the end of the relevant period) who have sideloaded a third party app during the relevant period	Indicator D is a flow measure of user response to the sideloading opportunity. It does not measure the % of apps that are sideloaded or the number of apps per user, but rather the proportion of users doing so.
	E. % of third-party apps (as a % of all third party apps sideloaded in the same period) for which sideloading was initiated but did not complete during the relevant period	Indicator E is similar to B but with respect to sideloading.
	F. % of active users (as a % of total users at the end of the relevant period) who initiated but did not complete sideloading a third part app in the relevant period who received (a) one gatekeeper message (b) two or more gatekeeper messages during the download process	Indicator F is similar to C but with respect to sideloading
	G. % of active end users (as a % of total users at end of the relevant period) who received an error message when seeking to use a gatekeeper app during the relevant period for each type of OS	Indicator G provides a benchmark against which to assess (in indicators H and I) the experience of third party apps that have been downloaded via other channels. In doing so it assumes that the majority of gatekeeper apps will either have been preinstalled or downloaded via the gatekeeper app store.
	H. % of active end users (as a % of users who have downloaded an app via a third party app store during the relevant period) who received an error message when seeking to use it during the relevant period	Indicator H measures the extent to which the user experience of apps which have been downloaded via a third party app store be inferior to that of apps which have been downloaded via the gatekeeper app store. Further

	I. % of active end users (as a % of users who have sideloaded a third party app during the relevant period) who received an error message when seeking to use the app during the relevant period	Indicator I measures the extent to which the user experience of apps which have been sideloaded may be inferior to that of apps which have been downloaded via the gatekeeper app store
	J. % of active end users (as % of total users at the end of the relevant period) who have downloaded and set third party applications as a default(s) during the relevant period	Indicator J is a flow measure of the ability and willingness of users to set downloaded third party applications as defaults, whether in response to prompts from third parties or otherwise.
	K. % of active end users (as % of total users at the end of the relevant period) who received a prompt from the third party in the same relevant period prior to setting the third party application as default(s) during the relevant period	Indicator K measures the impact of prompts on default setting by users (both frequency and effectiveness). There is, however, a question of whether the gatekeeper could measure this.
	L. % of active end users (as % of total users at the end of the relevant period) who have sideloaded a third party application and who have set it as a default during the relevant period	Indicator L is a stock measure of the ability and willingness of users to set downloaded third party applications as defaults (whether downloaded in the relevant period or previously). Indicates cumulative impact of measures on contestability.
	M. % of active end users (as a % of total users at the end of the relevant period) who have sideloaded a third party app store during the relevant period	This and the following indicators repeat indicators D -L but with respect to third party app stores rather than third party applications
	N. % of third-party app stores (as a % of all third party app stores sideloaded in the same period) for which sideloading was initiated but did not complete during the relevant period	
	O. % of active users (as a % of total users at the end of the relevant period) who initiated but did not complete sideloading a third party app store in the relevant period who received (a) one warning message (b) two or more warning messages during the download process	
	P. % of active end users (as % of total users at the end of the relevant period) who have downloaded and set third party app store as a default during the relevant period	

	Q. % of active end users (as a % of total users at the end of the relevant period) who received a prompt from the third party in the same relevant period prior to setting the third party app store as default R. % of active end users (as a % of total users at the end of the relevant period) who have sideloaded a third party app store and who have set it as a default during the relevant period S. % of active end users (as a % of total users at the end of the relevant period) who received a prompt from the gatekeeper in the same relevant period prior to setting the gatekeeper's app store as default T. % of active end users (as a % of total users at the end of the relevant period) who received a prompt from the gatekeeper in the same relevant period prior to setting the gatekeeper's application as default	Indicators S and T provide benchmarks of the effectiveness of gatekeeper prompts for users to set defaults against which to assess indicators K and Q
Art 6(5): non-discriminative ranking	% of first [3] search results displayed (i.e. impressions) that feature a gatekeeper URL during the relevant period (as an average of all search results displayed during the relevant period)	This provision aims to prevent unfair self-preferencing in ranking and related indexing and crawling. The proposed indicator measures the likelihood of gatekeeper URLs appearing in top 3 search results in a relevant period. It allows assessment of impact of changes in algorithms over time.
Art 6(6): switching between services accessed via CPS	N/a	The aim of this provision is to remove any restrictions on switching between services and applications provided via the CPS. It is possible to propose indicators that measure the % of end users who switch applications in a relevant period, but barriers to switching are more likely to be identified by users on a case by case basis.

Art 6(7): access to same hardware and software features	A. % of requests for access to gatekeeper hardware or software features from business users or alternative providers that are rejected/blocked on grounds of protecting integrity in the relevant period (by CPS) in the relevant period B. % of hardware and software features to which access is provided by the gatekeeper that are utilised by business users or alternative providers at the end of the relevant period	The aim of this provision is to require the gatekeeper to provide non-discriminatory access to the same software and hardware services that it makes available to itself via the OS or virtual assistant. Some of this will likely be complaints-driven and assessed on a case by case basis, but two indicators are proposed. Indicator A measures the extent to which the obligation to provide access is being inhibited by the gatekeeper on the grounds of protecting the integrity of the gatekeeper' services. It allows assessment over time and comparison between gatekeepers but does not assess the validity of such decisions or their justification. Indicator B is a stock measure of the response of third parties to the opportunity to access gatekeeper features and thus the impact of the provision on contestability.
Art 6(8): data for advertisers and publishers to verify ad performance on CPS	A. % of advertisers (as % of all advertisers) undertaking their own independent verification of the performance of the ad inventory on the relevant CPS at the end of the relevant period B. % of advertising revenue ((as % of all advertising revenue) represented by advertisers undertaking their own independent verification of the performance of the ad inventory on the relevant CPS at the end of the relevant period C. % of publishers (as % of all publishers) undertaking their own independent verification of the performance of the ad inventory on the relevant CPS at the end of the relevant period D. % of publishing remuneration (as % of all publisher remuneration) represented by publishers undertaking their own	This provision requires gatekeepers to provide information to advertisers and publishers on request in order to enable them to independently assess the performance of ad inventory (rather than rely upon the gatekeeper's own assessment) Indicator A is a stock measure of the use of performance measurement tools which the gatekeeper is required to provide to advertisers Indicator B is similar to A but measured by reference to advertising spend rather than advertisers Indicator C is similar to A, but applies to publishers rather than advertisers Indicator D is similar to C but measured by reference to publisher remuneration rather than publishers.

	independent verification of the performance of the ad inventory on the relevant CPS at the end of the relevant period	
Art 6(9): portability of end user data	A. % of active end users (as % of total end users at end of the relevant period) requesting data portability during the relevant period B. % of active end users (as % of total end users at end of the relevant period) who cancel data portability during the relevant period C. % of active end users (as % of end users who have requested data portability during the relevant period) that have data portability implemented at the end of the relevant period	The aim of this provision is to enable end users to require gatekeepers to share data with or port data to third parties Indicator A is a flow measure of user response to data porting opportunity. Allows assessment over time. Indicator B is a crude measure of the effectiveness of the porting process which may indicate user dissatisfaction with porting arrangements or the ease of cancellation (which may itself contribute to higher user uptake) Indicator C is stock measure of the cumulative effect of A and B
Art 6(10): portability of business user data	A % of active business users (as % of total business users at end of the relevant period) requesting portability during the relevant period. B.% of active business users (as % of business users who have requested data portability during the relevant period) that have portability implemented at the end of the relevant period C. % of requests by active business users during the relevant period for which active end users have provided consents to share personal data during the relevant or immediately prior period	The aim of this provision is to enable business users to require gatekeepers to share data with third parties, subject to consent by end users for the sharing of personal data Indicator A is a flow measure of business user response to data portability opportunity. Allows assessment over time. Indicator B is stock measure of business user response and of the overall impact of the provision. Indicator C is a measure of end user responses to the consent mechanism and effectiveness as well as a crude indicator impact of measure on contestability. Allows assessment over time including impact of changes to consent mechanism.

Art 6(11): Sharing data with online search engines	A. Number of requests for data from online search providers received by the gatekeeper during the relevant period B. % of requests received from online search providers in all periods that have been fulfilled at the end of the relevant period C. Total volume [or value] of data shared with online search providers during the relevant period for each of (a) ranking (b) query (c) click and (d) view data	The aim of this provision is to enable rival search engines to access ranking, query, click and view data held by the gatekeeper Indicator A measures rival search engine responses to the data access opportunity and allows assessment over time Indicator B is a stock measure of implementation of the data sharing measure by the gatekeeper Indicator C is a measure of the impact of the provision for each of the categories of data that may be requested. Allows assessment over time.
Art 6(12): FRAND obligations	A. % of active business users (as % of business users seeking access to gatekeeper services during the relevant period) who have raised a dispute for resolution during the relevant period B. % of complaints received by the gatekeeper during the relevant period or immediately prior period that are resolved at end of the relevant period.	This provision requires gatekeepers to deal with business users on FRAND terms and to provide for resolution when disputes arise. Whether terms offered are FRAND or not will likely requirement assessment on a case by case basis and is not susceptible to measurement by output indicators. Measures to assess the effectiveness of dispute resolution are proposed below. Indicator A may indicate the extent to which terms offered by the gatekeeper are considered FRAND by business users, as disputes suggest that those raising a dispute do not consider them so. Indicator B is a measure of the speed and effectiveness of the dispute resolution process. Guidance will likely be required on what 'resolved' means in this context
Art 6(13): no barrier to termination of CPS	A. % of active end users (as a % of total end users at end of prior relevant period) who terminate their CPS during the relevant period	This provision aims to ensure that end users can terminate their CPS without undue difficulty if they wish. Indicator A measures ability of end users to terminate and the impact of the provision

	B. % of active end users (as % of total end users at end of the prior relevant period) who request to terminate their CPS during the relevant period but had not done so at the end of the same period	Indicator B is a measure of potential obstacles or delays which users may face in terminating the CPS
Art 7: interoperability		This provision enables gatekeeper services to interoperate with those of other providers, upon their request, thereby allowing end users of each to communicate with each other.
	A. Number of requests for interoperability between individual users received by gatekeeper in the relevant period	Indicator A measures the response of other providers to the opportunity to interoperate
	B. % of requests received in the relevant period and prior [two] relevant periods that have been fulfilled at the end of the relevant period	Indicator B measures the rate at which requests are fulfilled by the gatekeeper and thus impact of the provision by reference to requests
	C. Total volume of text messages passing between the gatekeeper CPS and third parties in respect of individual users at end of the relevant period	Indicator C is a measure the impact of the provision by reference to the volume of communications passing between platforms at a given point in time
	D. % of text messages (as % of total volume of text messages send and received by individual active end users of the CPS) that pass between the gatekeeper CPS and third parties	Indicator D is a measure of the response of end users to the opportunity to communicate across platforms and the extent to which they do so
	E. As above for texts within groups of individual users	Applies indicators A-D to group texting
	F. As above for (a) messages with attached files (b) voice calls (c) video calls when obligation applies	Applies indicators A-D to other communications services as required by the provision.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank