

Consultation on the template for compliance report under the DMA

Fields marked with * are mandatory.

Please fill your details and input/upload your contribution at the bottom of this page.

The Commission is consulting on the template for the compliance report that designated gatekeepers will have to submit annually under Article 11 of the Digital Markets Act ('DMA').

Gatekeepers will be required to provide the Commission with their first compliance report within six months of their designation as gatekeepers. They will then be required to update these reports annually.

With the published consultation, the Commission is seeking feedback on the draft template that specifies the minimum information that the Commission expects gatekeepers to provide in their compliance report.

The gatekeeper's compliance reports will play an important role in enabling the Commission to verify that the gatekeepers comply with the obligations and prohibitions set out in Article 5, 6 and 7 of the DMA and that the measures implemented by the gatekeepers are effective in achieving the objective of the DMA. Where necessary, the Commission can make use of its investigatory and enforcement powers to ensure effective compliance with the DMA.

Target Group

All citizens, companies and organisations are welcome to contribute to this consultation. Contributions are sought particularly from undertakings, which are potential gatekeepers under the Digital Markets Act, as well as business users and end users of the potential gatekeepers and associations representing these users.

Objective of the consultation

The objective of the consultation is to gather comments on the draft template for the compliance report to be submitted by gatekeepers under Article 11 of the DMA.

In particular, the Commission would welcome feedback on the following two items:

- Precise indicators that the Commission could use to assess whether the measures implemented by the gatekeepers to ensure compliance are effective in achieving the objectives of the DMA and of the relevant obligations as required by Article 8 of the DMA; and
- content and presentation of the non-confidential summary of the compliance report that the gatekeepers must provide pursuant to Article 11(2) of the DMA in order to ensure that the summary enables third parties to provide meaningful input to the Commission on the gatekeeper's compliance with its obligations under the DMA.

The stakeholders' feedback will enable the Commission to prepare a finalised version of the template. The Commission may regularly update this template to request further information, which it expects gatekeepers to provide.

How to provide feedback

Please submit your contribution by 5 July 2023 (midnight). Your submissions should not include any confidential information. Your non-confidential submissions will be published on the Commission's website for the Digital Markets Act.

Your answers can be in any EU language.

Template for the compliance report

[DMA template - Compliance report consultation.pdf](#)

Your details

* Publication of your details

- ☒ I agree to the publication of my details along with my contribution
- ☐ My contribution should be published anonymously.

Privacy statement

[Consultation on DMA compliance report template privacy notice.pdf](#)

* Your first name

* Your family name

* Your organisation

* Your email address

Your contribution

You can insert a text and/or upload your contribution.

Type in your contribution (3000 characters maximum)

3000 character(s) maximum

Please upload your contribution.

854d5a16-6e50-4862-92e4-0f4e78934557

**/Comments_on_the_template_for_compliance_report_under_the_DMA.docx -
_Comments_on_the_template_for_compliance_report_under_the_DMA.docx.pdf**

Contact

EC-DMA@ec.europa.eu

Comments on the template for reporting pursuant to Article 11 of Regulation (EU) 2022/1925 (Digital Markets Act)

About the coalition

The Coalition for Competitive Digital Markets¹ represents 50+ companies from 16 countries (12 EU Member States) as well as the European DIGITAL SME Alliance, a business association made of more than 45,000 digital SMEs. Our goal is to promote competition in digital products and services.

The adoption of the Digital Markets Act (DMA) by the European Union is a huge step forward in favour of European SMEs as well as end-users' freedom, data ownership and control. If implemented and enforced right, the DMA has the potential to make the Internet ecosystem more balanced and competitive.

The Coalition for Competitive Digital Markets believes that leveraging the knowledge and experience of third parties, such as gatekeepers' existing and possible competitors, is critical to ensure proper implementation of the DMA. Therefore, we would like to provide our comments on the template for reporting pursuant to Article 11 of Regulation (EU) 2022/1925 (Digital Markets Act) (Template).

Suggestions to the Template

Overall we consider that the Template is very comprehensive, however, we would like to suggest adding the following:

- a) There should be a requirement for gatekeepers to provide a visual demonstration (a step by step visual guide/proof of concept) that would showcase the practical implementation of an obligation in question. Gatekeepers should provide a recorded demonstration and documentation with explanatory screenshots

¹ <https://competitivedigitalmarkets.eu/>

showcasing in an easily understandable way how certain obligations (in particular obligations related to end user or business user experience) would work in practice. This could be required but not limited to such obligations as tying and bundling, data portability, user switching, default setting, interoperability, *etc.*

For example, in case of self-preferencing via tying and bundling, the untying and/or unbundling may only be effective if an end-user's (or business user's) experience is not artificially degraded by the gatekeeper via different means such as dark patterns, the timing and number of actual steps necessary for a user to switch services, *etc.*

Another example would be for the case of interoperability (Article 7 of the DMA), where having a proof of concept showing interoperability between the gatekeeper and a third party would prove that the gatekeeper's approach is actually implementable in an easy enough manner by third parties requesting interoperability.

The goal of such a requirement would be to enable third parties and the European Commission to essentially receive a visual and easily understandable material that would reflect the implementation of the DMA's obligations while the rest of the gatekeepers' compliance report would serve as a written manual. Given that by the time the gatekeepers would have to submit their compliance reports they would also have to be compliant with the DMA's obligations, such a requirement would not be much of an additional burden to gatekeepers.

- b) The non-confidential summary of the gatekeepers' compliance report should be as comprehensive as possible to make sure that it provides a real and effective opportunity for third parties to understand and assess the implementation of an obligation in question and its effectiveness. We believe that the non-confidential summary of gatekeepers' compliance report should include the information indicated in point a) of this document (visual material) to make sure that any interested third party could easily understand the practical implementation of an obligation in question.
- c) Some of the provisions of Articles 5, 6 and 7 of the DMA require the gatekeeper to establish certain forms of access to their systems (e.g., interoperability) that

are meant to be used neither by end-users nor by business users, but by third parties, often competitors. The information list provided in point 2.1.2. of Section 2 (pages 3-4) of the Template does not include a requirement to specify how this access will be granted, and under which conditions this access could be granted. While this could be covered under point 2.1.2. h), we believe that this requirement deserves to be explicitly included. We therefore suggest adding the following additional requirement to point 2.1.2.:

“When compliance requires granting third parties (such as competing apps or service providers) access to data, interfaces or other technical features of the service, how will these third parties obtain such access, under which terms and conditions (including but not limited to how often these interfaces will be updated; how updates will be communicated; the committed level of service/uptime, the security disclosure process, etc.); how will the existence of this access and the necessary information for its practical use be made public; a link to the public documentation of this access and any other related information to allow the assessment of its practical feasibility.”

- d) For the provisions of Articles 5, 6, and 7 of the DMA that require gatekeepers to establish certain access to their systems as indicated above, the list of information mentioned in point 2.1.2. should also include a requirement for the gatekeepers to provide the European Commission with the results of any consultation with third parties that may use these accesses.

This is particularly important for the interoperability clause of Article 7 of the DMA. If the gatekeeper exposes an interface that cannot be realistically used by third parties (e.g., such an interface is technically not feasible), the interoperability clause of Article 7 would not be implementable in practice. Therefore, requiring the gatekeepers to demonstrate that they have worked with/consulted relevant third parties and addressed their needs would vouch in favour of the technical viability of the solution.

- e) We would also recommend expanding point 2.1.2. k) to request proof from gatekeepers that proper research on existing open standards and state of the art measures or implementations was made. The gatekeepers should have an obligation to justify in detail why such open standards and state of the art

measures and implementations were not chosen. Gatekeepers should also provide the European Commission with a plan to move towards such open standards and state of the art measures and implementations when relevant.

This would particularly help to ensure that the interoperability clause is implemented in the best spirit of the DMA. Indeed, end-to-end encrypted interoperability can be achieved between two services if gatekeepers open their APIs, but, as a consequence, that would:

- (i) increase the load on small businesses trying to interoperate with them, since SMEs would have to implement as many different APIs as gatekeepers they would try to connect to;
- (ii) make implementations more fragile, insecure and expensive;
- (iii) not work for end-to-end encrypted group communications due to the lack of common language.

This is why open standards, like IETF MLS (RFC9420), Matrix (<https://matrix.org>) and the work of IETF's MIMI working group, are necessary to realise the full potential of effective interoperability under Article 7 of the DMA. Therefore, we recommend the following wording of point 2.1.2. k):

“generally, any alternative measures whose feasibility or implications have been assessed and the reasons for not choosing them; and, in particular, where relevant (e.g., for interoperability), the results of the evaluation of existing open standards and/or state of the art implementations, the reason for not selecting them in case they were not chosen, and a high level plan to move towards such existing open standards for the next milestones.”

List of our Members

 abilian <small>CONNECTED, WE WORK!</small> Abilian (France)	 AICO <small>SOFTWARE</small> AICO EDV-Beratung (Austria)	 Alinto Alinto (France)
 Arawa (France)	 ARTABRO <small>TECH</small> ArtabroTech (Spain)	 Artellando <small>e-soluciones</small> Artellando e-soluciones (Spain)
 BEARSTECH Bearstech (France)	 benno MAILARCHIV Benno MailArchiv (Germany)	 BlueMind BlueMind (France)
 CR CapOne Research (Spain)	 CLUlife Cluplife (Germany)	 Collabora Collabora (United Kingdom)
 DASHLANE Dashlane (France)	 DHH <small>HRVATSKA</small> DHH (Croatia)	 eCorp eCorp (France)
 ECOSIA Ecosia (Germany)	 EGroupware <small>SMART ONLINE OFFICE</small> EGroupware (Germany)	 element Element (United Kingdom)
 European DIGITAL SME Alliance European DIGITAL SME Alliance	 FRANCELABS Datafari <small>Enterprise Search</small>	 GoFAST <small>by CEO-VISION</small> CEO-Vision-GoFAST

(Belgium)	FranceLabs (France)	(France)
 Greensoft Ltd (Romania)	 Halless (Italy)	 Hideas (Italy)
 idcert (Italy)	 Infomaniak (Switzerland)	 Input Objects (Germany)
 Iodé (France)	 Liberbyte (Germany)	 Logilab (France)
 Iterative Explorations (Belgium)	 Mailfence (Belgium)	 Mailo (France)
 Meetecho (Italy)	 Mojeek (United Kingdom)	 nablenet (Germany)
 Nextcloud (Germany)	 Nightingale HQ (United Kingdom)	 Open X-change (Germany)
 Omnis Cloud (Luxembourg)	 PaloServices (Greece)	 Photoprism (Germany)
 PowerDNS (The Netherlands)	 Proton AG (Switzerland)	 Proventa (Germany)

 RENVIS <small>RESEARCHING VISIONS</small> RENVIS (Greece)	 seeweb Seeweb (Italy)	 Smarthink Smarthink (Italy)
 STARTIN'BLOX Startin'Blox (France)	 StartMail StartMail (The Netherlands)	 Startpage StartPage (The Netherlands)
 tanaza Tanaza (Italy)	 Tutanota [®] Tutanota (Germany)	 univention be open. Univention (Germany)
 UNIVRSES Univrses (Sweden)	 VIVALDI Vivaldi (Norway)	 X-WIKI XWiki (France)
 yelp Yelp (United States)	 YouChoose ^{AI} YouChoose AI (France)	 ZEXTRAS Zextras (Italy)