Kluwer Competition Law Blog

Microsoft’s Second DMA Compliance Workshop – The Power of No: Maturing and Progressing on the DMA Journey

Alba Ribera Martínez (Deputy Editor) (University Villanueva, Spain) · Monday, June 23rd, 2025

The Digital Markets Act (DMA) became entirely applicable on 7 March 2024 for most gatekeepers. By then, the gatekeepers issued their compliance reports documenting their technical solutions and implementation of the DMA’s provisions under Article 11 DMA as well as their reports on consumer profiling techniques as required under Article 15 DMA. A year later, six gatekeepers submitted an update to the first version of their compliance reports (they can be found here).

As I did last year through The Power of No series, I will be covering this year’s compliance workshops held by the European Commission, where the gatekeeper representatives meet stakeholders to discuss their compliance solutions to the DMA’s obligations (and the updates they introduced since 2024). This blog post covers the first workshop organised by the EC in 2025, targeting Microsoft’s technical implementation of the regulation.

Regulatory dialogue with the European Commission

As opposed to last year’s compliance workshops, the EC was a bit more open in terms of disclosing some of the terms and content that it is currently discussing with the gatekeepers. At the start of the workshop, EC officials quickly went through the main points of dialogue that it is currently discussing with Microsoft regarding its compliance with the DMA. On that note, the EC highlighted its focus on Microsoft’s implementation of Articles 5(2), 6(9), 6(10), 6(3), and 6(7) DMA. In other words, these are the EC’s regulatory priorities to take Microsoft to an effective enforcement scenario.

For instance, the regulator stressed its focus on Microsoft’s introduction of new AI features on its two core platform services (CPSs), Windows PC OS and LinkedIn, insofar as those could be at odds with some of the regulation’s prohibitions, notably that of combining and cross-using personal data across services as set out in Article 5(2) DMA. Microsoft went into detail throughout the workshop to try to satisfy the EC’s thirst for covering all the AI grounds that have not been formally addressed by any other piece of EU regulation.

In this same sense, the EC underscored one of its top priorities in terms of the data portability solution (aka Article 6(9) DMA): Microsoft’s future release of Recall, a functionality termed by the gatekeeper as the ‘photographic memory for Windows’ integrated into Copilot+ PCs running on Windows 11. That is to say, Recall will not be available on every single device running on Windows PC OS, but only on Copilot+ PCs, which are specifically designed for performing AI tasks with additional computing power that outpaces Intel and AMD laptops. The Recall feature takes images of the user’s active screen every few seconds to record (or recall) all its past activities, including sensitive data and passwords. Upon the live recording of one’s screen, the user will then be able to transcribe and translate video meetings or search what they were viewing at a particular point in time by scrolling through a timeline of snapshots. Recall is already available in other jurisdictions of the world, such as the US, although it was forced to hold back its release after security concerns were raised ahead of its debut in June 2024. Some commentators even labelled the functionality as spyware, although Microsoft defended that Recall only stores data locally on the user’s PC and is protected by a PIN and not in the cloud. Due to the backlash, Microsoft also made Recall uninstallable on Copilot+ PCs and transformed it into an opt-in experience for the users to choose whether they wanted to enjoy the ~~(surveillance)~~ experience. The feature will not be available in the EU until later this year, as some reports confirm.

Surprisingly, the EC declared it was not analysing the Recall feature in the context of the data-related obligations of Articles 5(2) or 6(2) DMA. Instead, it is seeking feedback on how data available to the Recall feature may be instrumentalised by third-party business users under the data portability solutions. The workshop participants also remained moot on the soon-to-be-released future, although its rollout may provoke tensions with the encryption requirements set out, for instance, in Article 7 DMA relating to horizontal interoperability relating to messaging services such as WhatsApp and Facebook Messenger. As some critics have already argued, the Recall feature undermines the security of encrypted apps like WhatsApp and Signal by storing anything shown on the user’s screen, including private messages. Additionally, cybersecurity experts have already demonstrated that guessing the PIN gives full access to all screen content (deleted or not), including sensitive conversations, images, and passwords. Once more, the DMA is set at a crossroads with data protection standards and cybersecurity risks to be factored into the regulatory mix.

Reporting on progress: data portability, access, and combinations

After the EC’s intervention setting out the stage for a convivial discussion between the gatekeeper and stakeholders, the gatekeeper went into the thick of it by presenting the changes that it had made since March 2024 relating to its compliance with some of the data-related obligations on its LinkedIn service, notably Articles 5(2), 6(9) and 6(10).

To demonstrate compliance with the prohibition of combining and cross-using personal data across its services, Microsoft representatives brought forward its LinkedIn consent moment that it had already included within its 2024 compliance report (pages 3-12 of the report). In line with the consent experience, LinkedIn informs users about the way in which it connects services and types of data to deliver its core services. According to Microsoft’s legal representatives, the DMA consent moment is particularly targeted at informing users about the different services it caters to them, i.e., LinkedIn, LinkedIn Jobs, LinkedIn Marketing Solutions, and LinkedIn Learning, since combinations of personal data can only occur based on the premise of the consumer’s consent. To this effect, stakeholders asked about the user adoption rates relating to the granting of consent and Microsoft’s representatives confirmed that a meaningful portion of EEA members agreed to the consent moments, but they also had seen non-minimal responses from a portion of LinkedIn members not granting consent or minimising the volumes of data they granted access to. Despite the vehemency of some stakeholders in their questions addressed to Microsoft relating to its testing of the consent moment, the gatekeeper established that it had conducted no testing on the prompt's language neutrality.

Some participants in the workshop also tried to test the waters resulting from the Cologne Higher Regional Court's ruling on the granting of interim measures, where it interpreted Article 5(2) DMA in the context of metering whether Meta's integration of data from its Facebook and Instagram services to its AI models. According to the Court, there was no fundamental tension with the DMA provision since there is no 'merging' of data because the gatekeeper does not combine data from user profiles on different services or from other sources with regard to a single, specific user. Participants in the workshop asked (by dropping references to Meta) whether Microsoft also considered that data combinations should apply for the same user, i.e., user profiles to be captured under Article 5(2) DMA. Microsoft's representatives did not deviate from their main line of argument but inadvertently confirmed that the prohibition on data combinations applies across end users, regardless of whether a user profile may be provided therein.

Furthermore, Microsoft introduced the GDPR consent moment that it launched in December 2024 to satisfy the Irish data protection authority's concerns in its processing of personal data under the data protection regulation, as set out in pages 3-10 of its 2025 compliance report. Both consent prompts overlap substantially in terms of the data they refer to. Microsoft settled that it honors user choices made across the two of them in those cases where conflicting decisions relate to the same group of data. Additionally, stakeholders called out the gatekeeper on its implementation of Article 5(2)(d), compelling it to not sign in end users to other services of the gatekeeper to combine personal data, to the extent that Windows PC OS users are automatically signed in to its cloud storage service OneDrive upon the installation of Windows 10 and 11 with a Microsoft account. Microsoft's legal representative defended the gatekeepers' practice, insofar as the automatic sign-in to OneDrive was not performed for the purpose of combining data, but rather to provide easier access to online storage, as it already set out on pages 19-20 of its 2024 compliance report.

Moving forward on the data front, Microsoft did not report any additional changes to its compliance approach regarding Articles 6(9) and 6(10), except for the few instances where it reiterated its promises of continuous improvement of its LinkedIn Member Data Portability API, in terms of the features available to business users. On this front, the gatekeeper did provide some tangible evidence of its progress on the implementation of both provisions, since as of last year, 921,000 API calls were completed successfully stemming from the API program designed for LinkedIn and more than 2 million API calls were conducted relating to those APIs aimed at granting access to business user data pursuant to Article 6(10) DMA. Stakeholders voiced their concern about the low response rates of those same APIs and the limitations imposed on business users relating to the number of calls they could direct at the same API. Microsoft legal representatives justified the initial problems with the rolling out the APIs due to the sheer volume and complexity of the data involved when it comes to the portability of its LinkedIn users' data. Nonetheless, they assumed the compromise to investigate undue delays in those response rates or delays caused by technical issues, as well as to increase call limits based on internal reviews conducted as a consequence of business user requests.

Default settings, interoperability, and an evolving compliance strategy

In the second half of the workshop, Microsoft went on to describe how it constitutes an open platform for developers.

In line with the requirements set out under Article 6(4), users can install an application or app store onto Windows PC OS from any source without payment or permission from it. Predominantly, those downloads do not happen on the Microsoft Store, the gatekeeper's own app store for its operating system, but on the Internet. In this respect, the gatekeeper's business model revolves around the third-party developers' control over the technical and commercial experience within their applications and application stores.

Having said that, Microsoft presented to the workshop assistants the changes it had recently introduced to comply with Article 6(3) DMA to the requisite legal standard that the EC had set out for it to comply with, as stemming from their informal exchanges. Most of those changes reproduced the announcement Microsoft had already made on the 2nd of June on its blog. During intense debate, Microsoft defended that the few changes it introduced this year to its DMA compliance report do not point to the idea that it did not comply with the regulation from the first compliance deadline, i.e., March 2024. Instead, the gatekeeper upholds its willingness to engage with the EC's feedback and accommodate its points of view to the greatest extent possible, bearing in mind its broader business model.

Following its engagement with the EC, Microsoft decided to make its Microsoft Store uninstallable, imitating Apple's example, whereby it promised to make its App Store uninstallable for all users. Similarly, Microsoft also decided to budge in terms of the way users can change defaults on Windows PC OS, specifically to address the unique situation of file and link types. In other words, the EC pressured the gatekeeper to make it easier for users to change their defaults not only directly on an application (e.g., a browser) but also through settings depending on the type of file concerned (e.g., a PDF or a JPG file).

To that end, Microsoft will start rolling out in July 2025 functionality to: i) ensure that users can set any given browser as the default for all file types, except for pdf files; ii) automatically pin the user's chosen default browser on the Taskbar and Start of its operating system, unless the user decides to unpin them explicitly; and iii) provide a separate control for pdf controller to set defaults for this file type via a one-click set default button. Stakeholders called for further action in this respect and asked whether Microsoft would consider re-designing its default settings to accommodate the establishment of browser defaults only through one click. The gatekeeper's reaction was slightly discouraging since Microsoft's view is that users should be able to set defaults through Settings so that they remain in control of every single change they perform on their devices.

Alternatively, Microsoft will cease prompting users to make its proprietary browser Edge a default when it is not opened on the user's screen by May 2025. Aside from satisfying the EC's expectations in unbundling all digital services in the broadest sense possible, these few changes may also contribute to appeasing the calls for the reversal of the non-designation decision issued by the EC of its Edge service, which is currently under appeal under pending Case T-357/24.

Notwithstanding, some participants of the workshop still questioned Microsoft on the default settings ingrained into S Mode, a version of Windows 11 designed for security and performance.

According to the S Mode requirements, users must move out of S Mode completely (and onto Windows 11) to take advantage of the change of default settings from Bing and Edge and thus, the DMA provisions do not apply to those laptops operating on this particular Windows 11 version. Microsoft's legal representatives clarified this aspect of their compliance approach by setting out that under 10% of the machines in the EEA operate on S Mode, and more than 80% of them switch out of S Mode. On one side, they argued, that if 80% of users manage to switch out of the version, that demonstrates that it is not unduly difficult to do so. On the other side, a different configuration of S Mode would undermine its ultimate purpose, which is to provide a Windows PC OS version directed at novice users with small leeway for its configurability on the end user side.

Workshop participants also circled back to Microsoft's compliance report, in particular to page 82, to question specific carve-outs to the default rule. Specifically, the compliance report states that "*some applications are designed to use a specific application that is not the default application because it may provide the user with a more consistent end-to-end experience or enable the use of new features that are supported by the chosen specific application*". Legal representatives clarified that only two Microsoft applications rely on its browser Edge, Microsoft Teams, and Outlook. Both of those have controls where the user will be prompted on whether to choose the default browser to view a particular link or to use Edge, since the latter provides innovative technology to, for instance, display Outlook side-by-side with Edge. In their own view, such a situation does not breach Article 6(3) DMA because users remain in control of what web browser to choose when clicking on a particular link.

In a similar way, Microsoft's technical implementation of the DMA also evolved with respect to its interpretation of the interoperability solution under Article 6(7) DMA. At the previous compliance workshop held in 2024, the gatekeeper unbundled the Taskbar on Windows 10 from its Bing search engine and its feed extensibility of the Windows 11 Widgets Board, formerly backed by Edge's browsing experience.

Taking a step further, Microsoft has fundamentally re-worked its approach to providing access to business users to its Windows Search (desktop functionality enabling the finding of files, apps, settings and web information) and Widgets Board (feature providing a collection of interactive elements providing quick access to information and actions from various apps and services) functionality. For Windows Search, it will enable third-party web search providers to power it and will operate a redesign of the functionality to ensure they are automatically enabled to do so upon their installation. Those changes, according to Microsoft's representatives, will be rolled out in June 2025. Moreover, the gatekeeper has eliminated restrictions on access to the Windows Search functionality, whereby only applications available on the Microsoft Store could be shown on it. Since May 2024, it has eliminated the main requirement for its shipping. Additionally, when users click links on Windows Search or in Widgets Board, they will no longer be opened on Bing (nor will they be prompted to reinstall Edge). Once the change is finally rolled out in July, the user's default browser will be opened as a consequence of the user's interaction with the gatekeeper's proprietary functionality on the desktop.

GenAI tools intersecting with the DMA provisions

If there is a buzzword that has been making the rounds relating to the DMA's enforcement, it is generative AI. I have discussed the matter extensively in a couple of papers (see here and here).

And the topic of AI has flooded the workshops' agendas, not only for Microsoft but across all gatekeepers.

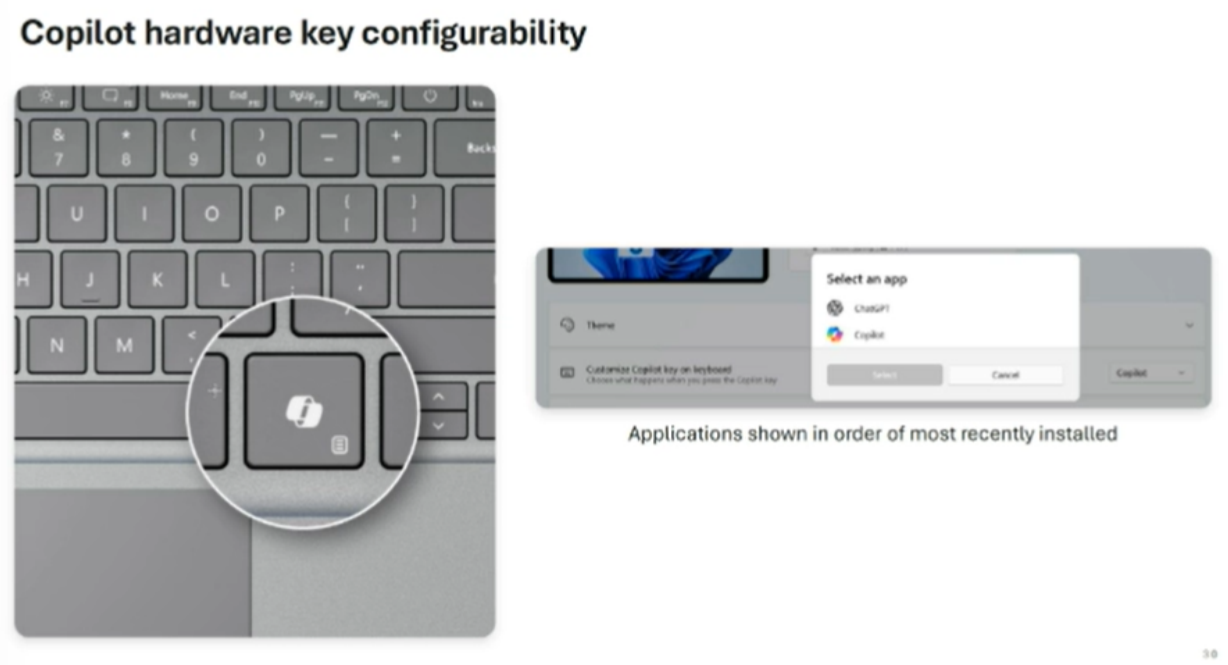
Microsoft's approach to metering the intersection between AI functionalities and the DMA has been quite distinct as opposed to the rest of the gatekeepers. In its 2025 compliance report, Microsoft already declared how it resolved the fundamental tension between Article 5(2) DMA and the generative AI-reliant tools it had introduced on its LinkedIn platform (pages 13-14), whereas other gatekeepers have preferred not to make any written disclosures to that effect. In this context, Microsoft already declared that to train its large language models (LLMs) to produce content and enhance its LinkedIn services, it had taken two immediate courses of action. First, it does not use EEA member data to train LLMs to generate content. Second, even in those cases where it was to do so, it would honour the EEA LinkedIn member's DMA consent settings for relevant data combinations. For instance, if an end user did not provide consent for combining personal data at the consent moment, that same data would lack a legal basis to be inputted into the LLM.

Although workshop participants tried to corner Microsoft into stating that it relied on the legitimate interest basis under Article 6(1)(f) GDPR to process personal data for the purposes of training and input data on its LLM, LinkedIn stood strong in defending that it did not use EEA member personal data for that purpose, so that it was not compelled to rely on any legal basis for justifying the processing of its personal data.

Despite a few references to AI made it to the Windows PC OS Annex to Microsoft's compliance report, the gatekeeper was eager to demonstrate how it would integrate AI solutions on Windows PC OS and how those would be regarded from the DMA perspective.

First, the gatekeeper's legal representatives reiterated that Windows operates as an open platform designed to deliver innovative and new applications. This same philosophy will apply to all AI applications running on Windows. Along these lines, it presented the two applications it runs on Copilot, its proprietary generative AI chatbot: Microsoft Copilot (for consumer scenarios) and Microsoft M365 Copilot (for work environments). Those applications run on Windows through public APIs that are available to any given developer, relying on its cloud infrastructure. In DMA terms, Microsoft has ensured that those APIs are available to all developers to build an app running on Windows. No further reference was made, however, to the dependency of these applications run by Windows with its own cloud infrastructure and cloud computing services, Microsoft Azure. It is yet unclear whether business users will be able to choose what cloud computing provider they choose to power their apps, even if they rely on Copilot, or if there is a technical bundle between both offerings.

Furthermore, Microsoft highlighted the creation of a new configurable keyboard key (the Copilot key) to make it easier for its users to launch an AI application when interacting with its Windows PC OS (see Image 1 below for reference).



Copilot hardware key configurability

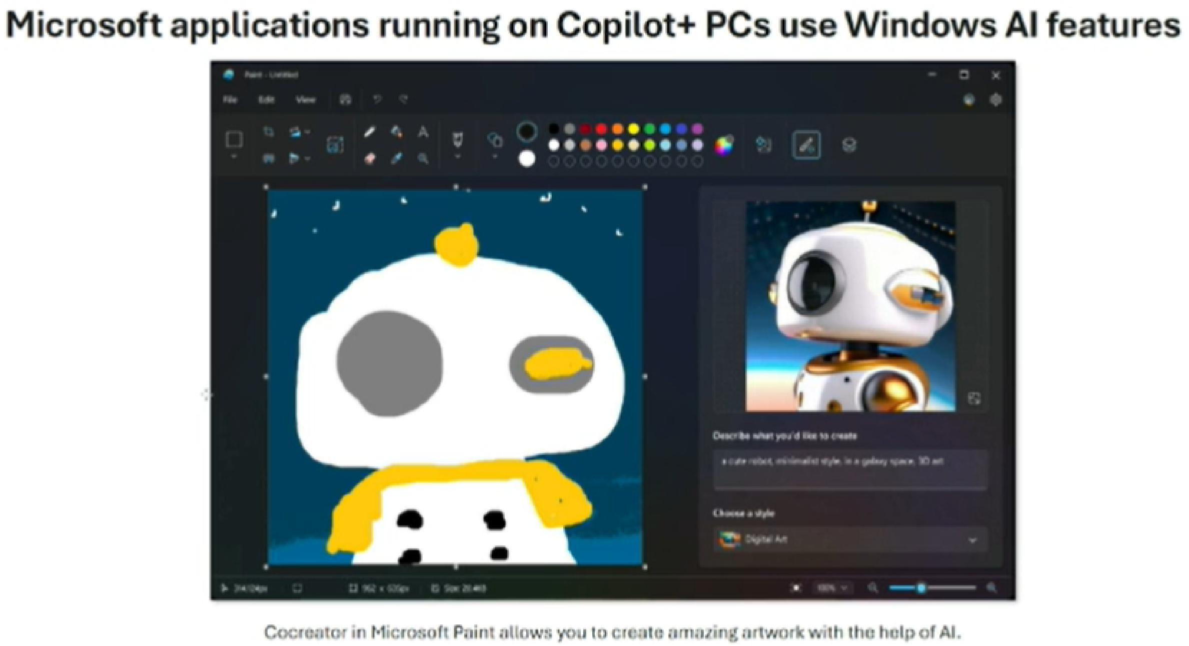
Applications shown in order of most recently installed

Select an app
ChatGPT
Copilot
Theme
Customize Copilot key on keyboard
Choose what happens when you press the Copilot key
Select
Cancel
Copilot
30

Figure 1. Screenshot of one of Microsoft's slides when presenting its AI functionalities.

According to the gatekeeper, when a user presses such a key, the operating system will redirect it to Copilot or, alternatively, to a competing AI service, as it already set out on page 123 of its compliance report. As shown in the screenshot above, the Copilot key currently shows the Copilot logo only. Asked by stakeholders, Microsoft reiterated that device manufacturers building PCs in the past have a long practice of including application-specific keyboard keys on their keyboards and, therefore, there would be no issue with the inclusion of a different logo on the key, notwithstanding the contractual requirements and specific restrictions that Microsoft might impose on such device manufacturers.

Second, Microsoft also put forward the platform APIs it offers to better build AI experiences on Windows. Most AI applications generally rely on AI models running on the cloud. However, the gatekeeper strives to establish a hybrid approach toward computing by building feasible solutions for AI experiences to run locally on the PC. As opposed to the dependence on the cloud infrastructure, running AI locally would keep data on-device, so that the exposure to data breaches would be reduced. Lower latency would be offered, therefore, ensuring faster and more reliable interactions with AI models. Correspondingly, Microsoft already includes on its Copilot+ PCs neural processing units designed to run AI models locally in an efficient way. On the side of expanding business user opportunities, it will additionally offer three key ways to run AI models locally by providing access to new APIs so that they can access the same type of hardware as Microsoft does. For instance, Microsoft is planning to release Foundry Local, enabling the local execution of LLMs directly on a Windows device via the download and customisation of open-source LLMs from an online catalogue on demand. In addition, it has already launched several local AI models part of Windows on Copilot+ PCs to process language and images, accessible to business users through publicly documented APIs. This provides the possibility for business users to enable AI capabilities without the need to find, run, or optimise their own proprietary model. To document the real-life results of these publicly documented APIs, Microsoft included a clear example to account for developer opportunities generated within its ecosystem.



Microsoft applications running on Copilot+ PCs use Windows AI features

Describe what you'd like to create

a cute robot, minimalist style, in a galaxy space, 3D art

Choose a style

Digital Art

Cocreator in Microsoft Paint allows you to create amazing artwork with the help of AI.

Figure 2. A screenshot of Microsoft's slides documenting API-based tools available to developers.

For this particular example, Microsoft shows how its proprietary Microsoft Paint running on a Copilot+ PC uses a custom model running on a neural processing unit. Specifications and documentation to access those same hardware features are made available to all developers via APIs.

In Microsoft's view, all these efforts demonstrate its readiness to comply by default and design. Nonetheless, it is yet unclear how those will work in terms of their bundling with other services and their reliance on its proprietary cloud infrastructure (which could be designated as a CPS at any given time by the EC through the qualitative process under Article 3(8) DMA).

Finally, Microsoft also set forth the features it will incorporate into Windows, relying on AI to deliver better functionality on its operating system, including examples such as Recall or Click to Do. Once again, it seems that the gatekeeper wants to provide the impression that it advances in the market in line with state-of-the-art technology, but that's simply not what the DMA is about. The regulation's devil is in the details, and the AI race is no exception to it.

To make sure you do not miss out on regular updates from the Kluwer Competition Law Blog, please subscribe here.

Now live
Global ESG Legal Compliance on VitalLaw®
Streamline compliance with ESG law and regulations with expert resources, global news updates, and legal research tools.
Wolters Kluwer
Learn More →

This entry was posted on Monday, June 23rd, 2025 at 9:00 am and is filed under AI, Digital competition, Digital economy, Digital markets, Digital Markets Act, European Union
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.