BEUC The European Consumer Organisation

The Consumer Voice in Europe

IMPLEMENTATION BY META, APPLE, GOOGLE, AMAZON, BYTEDANCE AND MICROSOFT OF THEIR OBLIGATIONS UNDER THE DIGITAL MARKETS ACT

BEUC analysis of non-compliance

Contact: Vanessa Turner and Sebastien Pant – competition@beuc.eu

BUREAU EUROPEEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2024-062 – 02/09/2024

Why it matters to consumers

The Digital Markets Act is a crucial piece of legislation to prevent Big Tech (gatekeepers) from controlling digital markets and to give consumers greater choice and protection. For example, Apple can no longer force consumers to use its payments system for in-app purchases on iPhones or iPads. Meta will have to provide the possibility for WhatsApp users to communicate with users of other instant messaging platforms. Alphabet/Google must actively ask consumers which search engine they want to use. It is crucial that the European Commission enforces this major legislation so that Big Tech companies comply and consumers reap the benefits of more open digital markets.

Summary

Apple, Meta, Alphabet/Google, Amazon, ByteDance and Microsoft have all been designated as 'gatekeepers' under the Digital Markets Act (DMA) and, in BEUC's view, are all currently failing to comply fully with this law to the detriment of consumers. We set out in this paper several ways in which we consider that these companies do not comply. It is important to note that this report is not an assessment of compliance with every single provision of the DMA, but instead covers the issues that are of most direct relevance to consumers (i.e. "end users" under the DMA). Examples of non-compliance with DMA rules from BEUC's perspective include:

***Meta**:*

1. ***Requiring consumers' consent to use their personal data across Meta services, including for online ads**. Meta uses misleading language and other harmful choice architecture to steer consumers towards allowing Meta to use their personal data across various services.*
2. ***Interoperability on instant messaging**. Meta's user interface plans for enabling consumers to communicate with users across WhatsApp/Messenger and other instant messaging services appear likely to undermine effective interoperability.*

Apple:

1. ***Enabling users to get better deals outside the App Store**. Apple employs non-neutral language to scare consumers away from choosing alternative payment services or subscribing to cheaper services outside the app, e.g. for music streaming.*
2. ***Choice screen for browser.** Apple's choice screen design is not compliant in multiple ways. For example, it fails to provide sufficient information to make an effective choice and* the *user journey through the choice screen is confusing, complex and creates negative friction.*
3. ***Changing default settings**. Apple does not make it easy for consumers to change their default settings.*
4. ***Downloading alternative app stores and apps**. Apple creates unnecessary steps to impede or deter consumers from switching to alternatives.*

Alphabet/Google:

1. ***Subscribing to services outside the PlayStore****. Alphabet/Google must not deter end users from taking up alternative, potentially cheaper services.*
2. ***Self-preferencing in general search results.*** *Alphabet/Google's redesign of its search results page has not eliminated Google's preferential treatment of its own services.*
3. ***Requiring consumers' consent to the use their personal data across Google services, including for online ads.*** *Google's user interface designs steer consumers to agree, rather than enabling them to make a freely given, informed consent choice.*
4. ***Choice screens for browsers and search engines, and easily changing defaults****. The choice screen designs and roll out of these have not been compliant. Google does not make it easy for consumers to change their default settings as the DMA requires.*

Amazon:

1. ***Requiring consumers' consent to use their personal data across Amazon services.*** *Amazon's user interface designs steer consumers to agree, rather than enabling them to make a freely given, informed consent.*
2. ***Self-preferencing in product search results****. Amazon must clearly demonstrate that it is not self-preferencing its own products to consumers.*
3. ***Unsubscribing easily from its services****. Amazon continues to use behavioural techniques that make it harder to unsubscribe from Amazon Prime than to subscribe.*

ByteDance:

Requiring consumers' consent to use their personal data across ByteDance services*. ByteDance uses behavioural techniques to steer consumers towards allowing ByteDance to use their data across various services.*

Microsoft:

Requiring consumers' consent to use their personal data across Microsoft services. *Microsoft's user interface designs raise concerns about consumers' ability to make freely given, specific and informed choices regarding the use of their data across various services.*

We ask the Commission to examine these issues carefully and to take the necessary steps to ensure full compliance by the gatekeepers.

Contents

1. Introduction 4

2. Meta. 4

2.1. Incomplete compliance report 4

2.2. Use of consumers' personal data 4

2.2.1. Facebook/Instagram with Meta Ads 5

2.2.2. Facebook with Instagram 6

2.3. Interoperability of other instant messaging apps with WhatsApp and Messenger 7

3. Apple 8

3.1. Inadequate compliance report and implementation delays 8

3.2. Enabling users to get better deals outside the AppStore 8

3.3. Choice screens to choose browsers and default settings 10

3.4. Downloading alternative apps and app stores 12

3.5. Use of consumers' personal data 12

4. Alphabet/Google 12

4.1. Subscribing to services outside the PlayStore 12

4.2. Self-preferencing 13

4.3. Use of consumers' personal data 13

4.4. Choice screens to change default settings (browsers and search engines) 14

4.5. Uninstalling apps 15

5. Amazon 15

5.1. Inadequate compliance report 15

5.2. Use of consumers' personal data 15

5.3. Self-preferencing 16

5.4. Termination conditions 17

6. ByteDance 17

6.1. Inadequate compliance report 17

6.2. Use of consumers' personal data 17

7. Microsoft 20

Use of consumers' personal data 20

8. Importance of testing end user interfaces and documentation on design choices 23

1. Introduction

The EU's Digital Markets Act imposes a set of obligations and prohibitions on designated digital "gatekeepers" in relation to their "core platform services" (e.g. social networks, app stores, search engines) with a view to making digital markets contestable and fair. This legislation is in large part a response to anticompetitive practices from major tech companies over the past years. If properly implemented and enforced, the DMA should bring consumers significant benefits in the form of more innovation and choice.

This paper summarises where, on the issues of most direct relevance to consumers, BEUC believes that Apple, Meta, Alphabet/Google, Amazon, ByteDance and Microsoft are failing to comply with the Digital Markets Act. It is based on more detailed submissions by BEUC to the European Commission on each of these companies.[1] These analyses were undertaken on the basis of the companies' DMA compliance reports and other publicly accessible information. This report is not an assessment of compliance with every single provision of the Digital Markets Act but focuses on key consumer-facing obligations.

It is essential that the Commission swiftly pursues non-compliance by gatekeepers so that the benefits of the DMA are realised for consumers.

2. Meta

2.1. Incomplete compliance report

The DMA (Article 11) requires gatekeepers to publish a non-confidential summary of their compliance report to enable third parties (including consumer representatives) to assess whether the gatekeepers comply with their obligations under the DMA. Meta's non-confidential compliance report does not follow the DMA's requirements, or the compliance report template adopted by the Commission. Meta's report includes no information on important issues for establishing compliance from the end user perspective, for example user interface design testing. This undermines the effectiveness of compliance reports and thus the ability of third parties to contribute to assessing Meta's compliance with the DMA and does not fulfil the requirements of Article 11 DMA.

2.2. Use of consumers' personal data

The Digital Markets Act (Article 5(2)) restricts gatekeepers from using consumers' personal data for advertising purposes and combining/cross-using consumers' personal data from a gatekeeper's core platform service (for example Meta's Facebook) with personal data from another of their services or with personal data from third party services, unless the end user has freely consented to this.

Gatekeepers have to offer consumers a choice which includes a less personalised but equivalent service if consumers do not wish to consent to the use of their data, and cannot make the use of the core platform service or certain of its functionalities conditional upon the end user's consent. The end user's choice must be freely given, specific, informed and unambiguous and cannot be undermined by behavioural techniques or user interface

[1] BEUC made submissions to the European Commission on Apple, Meta and Google in May 2024 and on Amazon, ByteDance and Microsoft in August 2024. This summary notes where these gatekeepers have announced changes to their DMA implementation since BEUC's submissions and where the Commission has opened investigations.

designs, including designs that are non-neutral, or that subvert end users' autonomy or decision-making on the use of their data (Article 13 anticircumvention clause).

Meta's choice screens on personal data use across its various services fail to comply with the DMA requirements. The way that Meta presents choices to users does not allow consumers to make freely given, specific, informed and unambiguous choices as required by Article 5(2). Meta also uses behavioural techniques and interface designs that are non-neutral and subvert the consumer's autonomy or decision-making choice contrary to Article 13.

Two examples of this are set out below but similar issues arise with Meta's other personal data use choice screens.[2]

2.2.1. Facebook/Instagram with Meta Ads

The choice screen Meta rolled out from November 2023 for Facebook and Instagram users to combine their personal data with Meta Ads (see Figure 1 below) breaches the DMA's requirements, by steering users towards Meta's preferred option instead of offering a freely given, specific, informed and unambiguous choice.

For example, neither the wording for the two options (*"use for free"* or *"subscribe")*, nor the colours (consenting is blue, while refusing is white), are neutral. Meta also uses language exploiting loss aversion bias "Your current experience" to steer users towards maintaining the status quo and also implies that consenting to the use of personal data is the default option.

Describing the consent option as *"Use for free"* is particularly misleading and can constitute an unfair commercial practice, due to the recognised economic value of personal data.

This "pay or consent" choice furthermore does not amount to a less personalised but equivalent alternative.

[2] These should be investigated in the context of the open investigation into Meta's implementation. See European Commission, Press release 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act' (25 March 2024); and European Commission, Press release 'Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act' (1 July 2024).

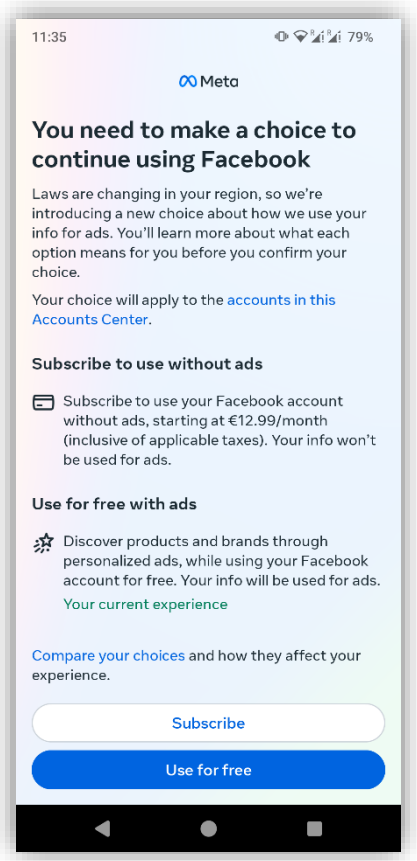

Figure 1: Screenshot of the Meta Ads choice screen

2.2.2. Facebook with Instagram

In relation to Facebook and Instagram, the choice screen presented to the consumer (see Figure 2 below) uses several design techniques which steer users to accept the data cross-use or combination option favoured by Meta rather than enabling a freely given consent choice.

- The colours of the various buttons to give or refuse consent are not neutral. The button to give consent is bright blue whereas the button to refuse it is transparent, thereby visually steering the end user to consent.
- The wording used on the buttons is not neutral. Instead of providing one option to "Consent"/"Accept" and another option to "Don't Consent" or "Refuse", the choice screen gives end users the choice between "Confirm", on the one hand, and "Manage accounts" on the other hand, which steers uses to "confirm".
- Meta uses the word "info" instead of "personal data" which many consumers associate with something that is worth protecting.
- Meta's language appears to use the well-known loss aversion behavioural bias to steer users towards maintaining the status quo ("Your experience stays the same").

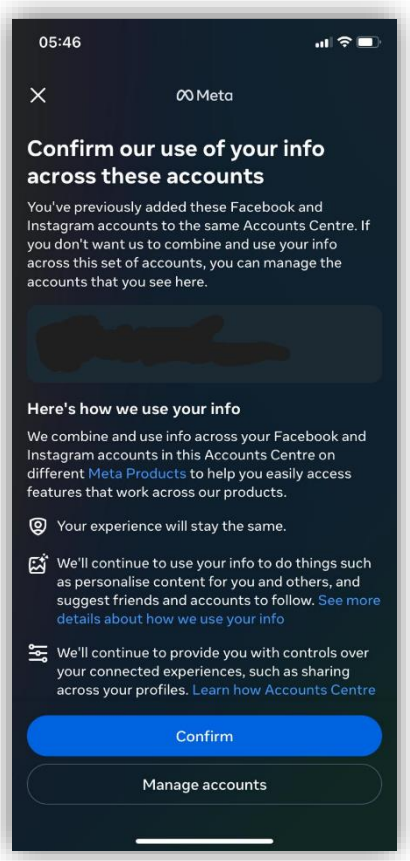

Figure 2: Screenshot of the Facebook/Instagram choice screen

2.3. Interoperability of other instant messaging apps with WhatsApp and Messenger

Meta is obliged under the DMA (Article 7) to provide interoperability between its messaging services (WhatsApp and Messenger) and the instant messaging services of third parties when requested and free of charge. This would, for example, allow users of alternative messaging services to communicate with WhatsApp users and vice versa.

Meta has not yet provided sufficiently detailed information about what the user interface for this interoperability will look like, nor details about how it will work. However, it will be essential that the user interface design and the messaging experience do not undermine consumers' desire to use these new possibilities. There are signs that this could be the case. Such an approach by Meta could not amount to compliance with Article 7 of the DMA.

The European Commission should carefully evaluate Meta's user interface design and proposed messaging experience and furthermore require Meta to provide any testing data and documentation underlying its user interface design to establish whether Meta's interoperability proposals comply with the DMA before they are rolled out.

3. Apple

3.1. Inadequate compliance report and implementation delays

As set out above, the DMA (Article 11) requires gatekeepers to publish a non-confidential summary of their compliance report to enable third parties (including consumer representatives) to assess whether the gatekeepers comply with their obligations under the DMA. The form, content and scope of Apple's compliance report are wholly inadequate and do not follow the DMA's requirements or the template of the Commission. Even with the cross-references to other documents, the level of detail does not allow third parties to analyse Apple's compliance as required by the DMA. Apple's report includes no information on important issues for establishing compliance from the end user perspective, for example user interface design testing. This undermines the effectiveness of compliance reports and does not fulfil the requirements of Article 11 DMA. Furthermore, there is no audited profiling report as required by Article 15.

In addition, Apple's compliance report announced multiple delays to its DMA implementation measures which would have a knock-on effect on consumers. These amount to blatant violations of the DMA.

3.2. Enabling users to get better deals outside the AppStore

The Digital Markets Act requires Apple to allow app developers to communicate and promote their offers, and conclude contracts with consumers free of charge outside the App Store (Article 5(4). The Commission has opened an investigation into this.[3] Article 5(7) prohibits gatekeepers from requiring app developers to use the gatekeeper's payment system for in-app purchases. Consumers thus have the right to buy their services though other channels than Apple's App Store and to use other payment systems than Apple's for in-app purchases.

Leaving aside non-compliance in Apple's business terms with app developers[4], Apple is not complying with its obligations in that it is scaring consumers away from choosing to subscribe to potentially cheaper services outside the App Store and from alternative payment systems for in-app purchases. As shown in Figures 3 and 4 below, the wording of the information/disclosure (or "scare") screens, which Apple requires app developers to use, is clearly designed to imply that alternative purchase or payment options to Apple's put consumers at risk, regardless of the factual situation.[5]

[3] See: European Commission, Press release 'Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple' (24 June 2024).

[4] Including Apple's latest communication to app developers see: Apple, Support - Apple Developer 'Alternative payment options on the App Store in the European Union' (8 August 2024).

[5] It is noted that in Apple's latest communication to app developers, the "scare screen" shown in Figure 3 has been revised and improved, though the full contents of the "user disclosure" is not visible in: Alternative payment options on the App Store in the European Union - Support - Apple Developer. No changes have been proposed for Figure 4.

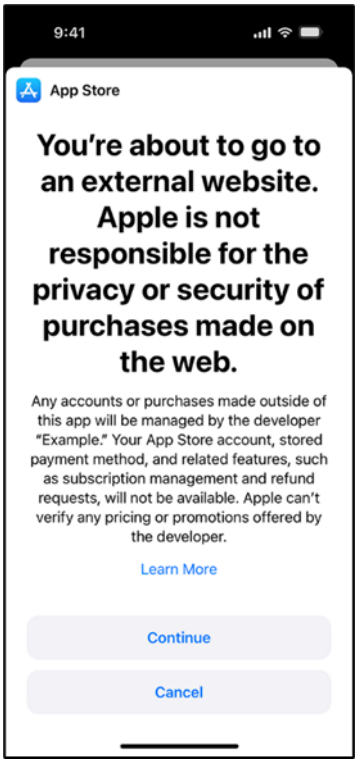

Figure 3: Apple's information screen for purchases outside the App Store

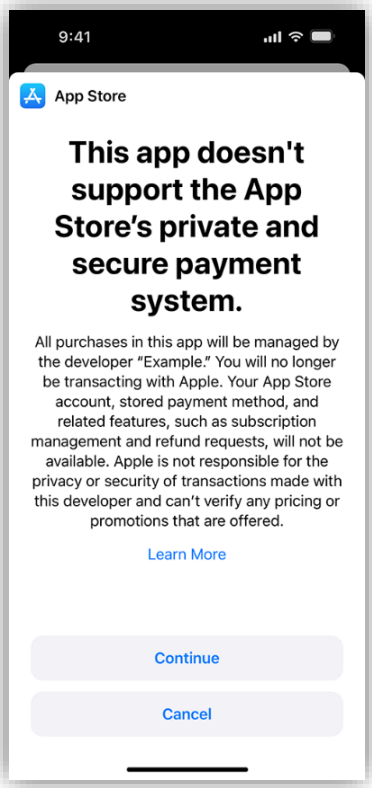

Figure 4: Apple's payment service information screen

Consumers are thereby deterred from considering potentially cheaper or better offers. These screens do not leave end users "free to choose" alternative offers of business users as required by the DMA (Recital 40), and amount to circumvention under Article 13 in that they are non-neutral and likely to subvert end users' autonomy, decision-making, or free choice.

3.3. Choice screens to choose browsers and default settings

The DMA requires gatekeepers to enable users to easily change their default settings on operating systems, virtual assistants or web browsers (Article 6(3) and (4)). It also requires that gatekeepers show end users a choice screen with the main available browsers to enable users to choose an alternative browser where the gatekeeper directs or steers users by default to their own browser (Article 6(3)).

Several aspects of Apple's browser choice screen design are not compliant with Article 6(3). Examples of these are set out below.[6]

The choice screen offers almost no information on the different browser options, no forced scroll before the consumer has to make a choice, and Safari is not systematically shown below the fold. These design elements are not in line with research on what constitutes an effective choice screen for consumers.

Furthermore, the user journey through the choice screen is confusing, complex and creates negative friction, as does when the choice screen is shown to consumers. Research has shown that such negative friction undermines the effectiveness of the choice screen and thus Apple's compliance.

If a consumer selects an alternative browser to Safari as their default browser, a shortcut to Safari nevertheless remains in the home screen dock (in the "hot seat") – see Figure 5 - which is where most consumers would typically access the internet. Although consumers can manually change this setting, it requires additional steps which are not required when they choose Safari as their default browser. This again undermines the effectiveness of the choice screen.

[6] These should be investigated in the context of the open investigation into Apple's implementation: European Commission, Press Release 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act' (25 March 2024.

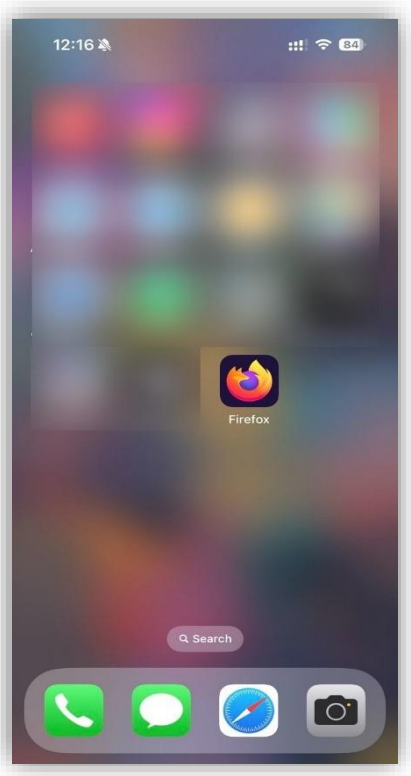

Figure 5: Safari must be removed manually from the dock.

Apple's compliance report states that Apple's measures to allow end users to easily change all their defaults are not yet complete. What Apple has done so far also does not amount to enabling end users to easily change their defaults as the DMA requires. For example, if consumers want to change their default browser at a point in time after the browser choice screen, they have to navigate to the iOS settings. The settings menu where the default browser can be changed is called 'Safari' instead of a neutral term like 'Browser App', even if the current default browser is not Safari. This is confusing and does not enable consumers to easily change easily their default settings as required by Article 6(3) and (4).

Apple also does not enable end users to easily uninstall apps. For example, Apple announced in its compliance report that the option to completely delete Safari from iOS will only be available by the end of 2024, whereas the obligation applies since 7 March 2024.

All of the above mean that Apple is not in compliance with its obligations under Articles 6(3) and (4).

On 22 August 2024, Apple announced changes to its choice screen, default apps and app deletion which appear to respond to several of the concerns set out above. These changes are due to be implemented "by the end of this year".[7] The precise details of these changes will need to be evaluated.

[7] https://developer.apple.com/news/?id=zqlax7qc

3.4. Downloading alternative apps and app stores

Article 6(4) requires Apple to allow end users to install and use alternative apps stores and to install apps other than through Apple's App Store. Leaving aside non-compliance in Apple's business terms with app developers and app stores, Apple has not provided any description or screenshots of the interface that consumers are presented with when they install an alternative app or app store. The analysis below is therefore based on public information sources.

The overall process of installing an alternative app store is complex and requires numerous unnecessary steps which are likely to impede or deter end users from switching to an alternative application store to Apple's App Store, thereby undermining the purpose of Article 6(4). There are furthermore reports online that, even after following these steps, there can be technical difficulties which prevent the installation of an alternative store.

On the basis of the above, Apple's implementation is not compatible with effective compliance under Article 6(4) and Article 13. The Commission's investigation into Article 6(4) must look closely into this.[8]

3.5. Use of consumers' personal data

The Digital Markets Act (Article 5(2)) restricts gatekeepers from using consumers' personal data for advertising purposes and combining/cross-using personal data from a core platform service with personal data from another of their services or with personal data from third party services, unless the end user has freely consented to this.

At the compliance workshop, Apple said that the only data in scope of the DMA was App Store data. No identifiable data was collected by iOS or Safari in line with data minimisation. Apple also said that it only has one advertising service in the EU which is search advertising in the App Store.

BEUC has not seen any Apple consent screens to support Apple's claims that it has put in place policies and approval mechanisms to ensure that any use of in-scope personal data complies with the DMA. We assume that the Commission will be verifying that there is indeed no use of personal data across services as Apple is not apparently seeking consumer consent for this pursuant to the DMA except in limited cases.

4. Alphabet/Google

4.1. Subscribing to services outside the PlayStore

The Digital Markets Act (Article 5(4)) requires gatekeepers to allow app developers to freely communicate with and steer consumers to offers outside app stores free of charge.

The Commission has already opened an investigation as Alphabet/Google imposes various restrictions on app developers.[9] This investigation must also cover user interface and information screens to ensure that these do not deter end users from taking up alternative

[8] See European Commission, Press release 'Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple' (24 June 2024).

[9] See: European Commission, Press release 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act' (25 March 2024).

offers by, for example, the use of "scare screens" or an overly complex user journey to take up alternative offers.

4.2. Self-preferencing

Under Article 6(5), the Digital Markets Act prohibits gatekeepers from treating their own products and services more favourably than those of third parties. This means Google cannot self-preference its own services or products in terms of what is displayed on its search engine results pages (SERP).

Google has been testing various new search results pages live. These do not appear to have eliminated self-preferencing by Google of its own services. To make sure Google complies with this provision, the Commission must obtain Google's testing data for the different search engine results page displays it has shown to end users recently and any future proposed design testing to see what this has done in terms of flows to Google's vertical search services (such as Google Shopping or Flights) compared to flows to competing similar service providers. [10] This should also be verifiable by third parties. The Commission must also obtain and analyse the documentation underlying the SERP design choices.

Compliance with Article 6(5) may mean some changes for end users who have been conditioned to see results in the way that Google wanted them to, which may lead to some consumer confusion. Short term inconvenience should not, however, trump the preservation of end user choice in the long term. Google has choices in how it implements this obligation and can ensure a positive user experience.

4.3. Use of consumers' personal data

As set out above, the Digital Markets Act (Article 5(2)) restricts gatekeepers from using consumers' personal data for advertising purposes and combining/cross-using consumers' personal data from a gatekeeper's core platform service (for example, Google's search engine) with personal data from another of their services or with personal data from third party services, unless the end user has freely consented to this.

Gatekeepers have to offer a choice which includes a less personalised but equivalent service if consumers do not wish to consent to the use of their data, and cannot make the use of the core platform service or certain of its functionalities conditional upon the end user's consent. The end user's choice must be freely given, specific, informed and unambiguous and cannot be undermined by behavioural techniques or user interface designs, including designs that are non-neutral, or that subvert end users' autonomy or decision-making on the use of their data (Article 13 anticircumvention clause).

In the case of personal data use for online advertising, it appears that Alphabet/Google plans to rely on the consent consumers are asked to give via cookie banners when using the website or application of a third party, instead of asking consumers for consent on Google's core platform services. The DMA, however, states that consent through third parties should be exceptional and only used if consent cannot be given directly to the gatekeeper's core platform service This has furthermore been found to be incompatible with the GDPR.[11]

[10] This could be done in the course of the Commission's open investigation, see: European Commission, Press Release 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act' (25 March 2024).

[11] "The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR" (https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-

In the case of cross-use/combination of personal data, Alphabet/Google's choice screen (see Figure 6 below), refers to "linking services", rather than cross-use/combination of personal data, and frames the consent request in a positive way rather than on the reality of personal data use, which is likely to steer end users to agree, rather than enable them to make a freely given, specific, informed and unambiguous choice. This would constitute a breach of Articles 5(2) and 13 of the DMA.[12]

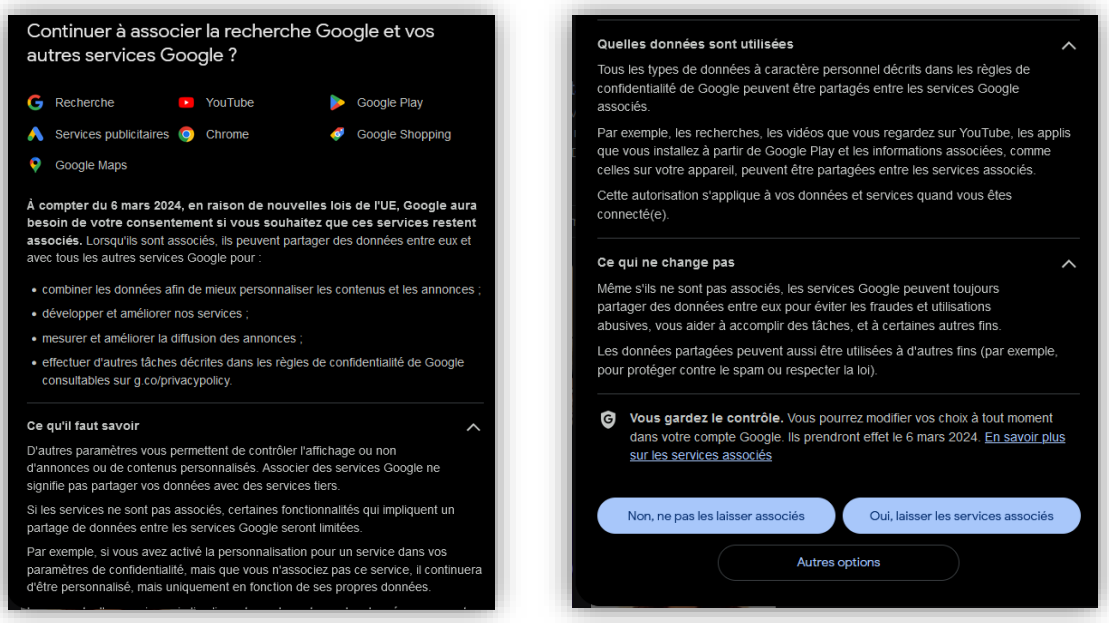

Figure 6: Screenshots in French of the Google choice screen

4.4. Choice screens to change default settings (browsers and search engines)

The DMA requires gatekeepers to enable users to easily change the default settings on their operating system, virtual assistant or web browser (Article 6(3) and (4)). It also requires that gatekeepers show end users a choice screen with the main available search engines and browsers to enable users to choose an alternative search engine or browser where the gatekeepers direct or steer users by default to their own search engine or browser (Article 6(3)).

Google's implementation of these requirements raises non-compliance and circumvention concerns in relation to some elements of the choice screen design, its delayed and incomplete roll-out (including limiting roll-out to Android Versions 13 and 14 when Versions 11 and 12 are still widely available and used by consumers), and in that Google effectively overrides the end users default choices through several design features.

mechanism-that-infringes-the-gdpr); Judgement of the Court (Fourth Chamber) in Case C 604/22 (https://curia.europa.eu/juris/document/document.jsf?text=&docid=283529&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=7063554).

[12] Alphabet/Google also used a design for this choice screen prior to 6 March which steered consumers even more to the company's preferred option and which used even less neutral language ("Keeping services linked" – implying that this should be the default). The Commission should clarify whether users were presented with a second choice screen if they had already consented using the pre-6 March version as this could amount to circumvention of Article 5(2).

4.5. Uninstalling apps

Gatekeepers must allow users to easily uninstall any apps on their operating system (Article 6(3)).

It appears, however, that apps such as Chrome, Search, Gmail, Maps, YouTube and Meet can only be deactivated, not uninstalled. This is not the same thing and should be considered non-compliant as it would not counter the harm to contestability and fairness of app pre-installation on Android devices and thus amount to effective compliance.

5. Amazon

5.1. Inadequate compliance report

As set out above, the DMA (Article 11) requires gatekeepers to publish a non-confidential summary of their compliance report to enable third parties (including consumer representatives) to assess whether the gatekeepers comply with their obligations under the DMA. Amazon does not follow the DMA's requirements, or the compliance template provided by the Commission. Amazon does not include information on important issues for establishing compliance from the end user perspective, such as how it designed and tested its end user interfaces. This undermines the effectiveness of compliance reports and does not fulfil the requirements of Article 11 DMA.

5.2. Use of consumers' personal data

The Digital Markets Act (Article 5(2)) restricts gatekeepers from using consumers' personal data for advertising purposes and combining/cross-using consumers' personal data from a gatekeeper's core platform service (for example, Amazon's Marketplace) with personal data from another of their services or with personal data from third party services, unless the end user has freely consented to this.

Gatekeepers have to offer a choice which includes a less personalised but equivalent service if consumers do not wish to consent to the use of their data, and cannot make the use of the core platform service or certain of its functionalities conditional upon the end user's consent. The end user's choice must be freely given, specific, informed and unambiguous and cannot be undermined by behavioural techniques or user interface designs, including designs that are non-neutral, or that subvert end users' autonomy or decision-making on the use of their data (Article 13 anticircumvention clause).

Amazon has created two choice screens for the purpose of Article 5(2). Neither appear to constitute effective compliance with its DMA obligations under Article 5(2) in conjunction with Recitals 36 and 37, and Article 13, in particular Article 13(4) and Article 13(6). Amazon uses behavioural techniques to exploit known biases, thus preventing users from making free, specific, informed and unambiguous consent choices.

Amazon's Store Prompt (see Figure 7 below) which is intended to seek consumer consent for data combination and cross-use illustrates this non-compliance.

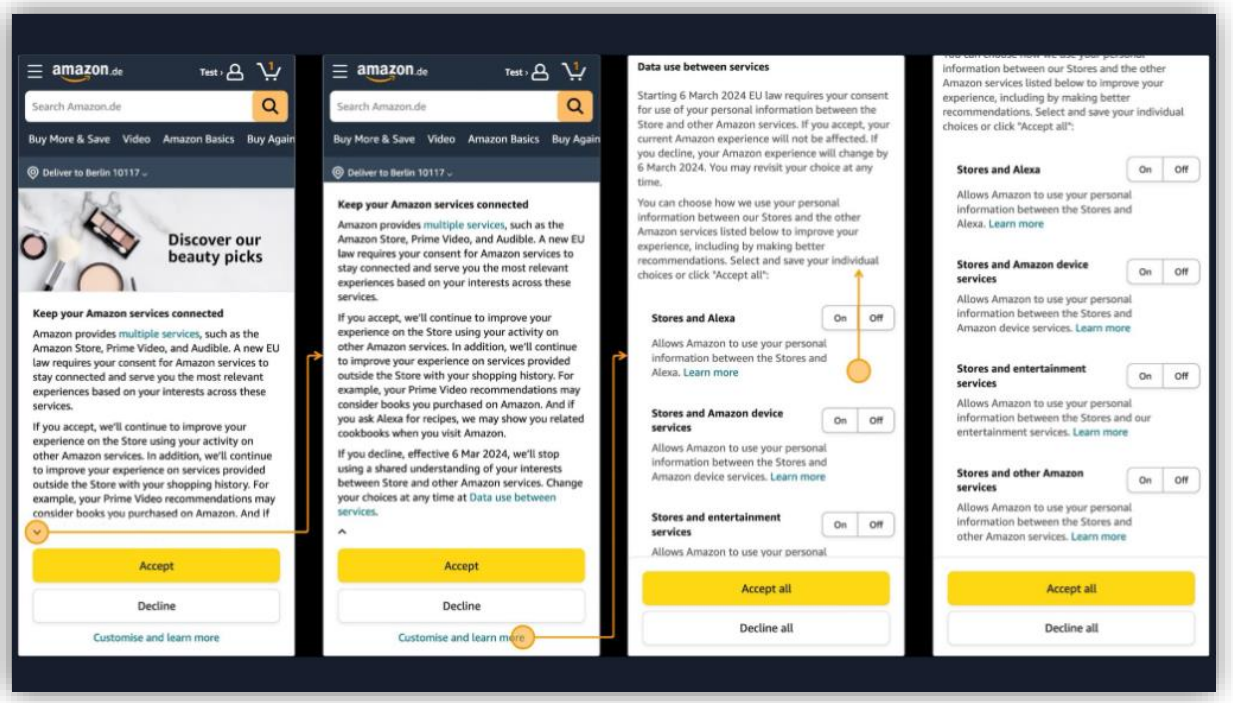

Figure 7: Screenshots of the Amazon store prompt

For example:

- The colour of the button to give consent is yellow whereas the button to refuse it is transparent. This behavioural technique can exploit end users' 'saliency bias', thereby visually steering the end user to consent to personal data combination and cross-use.
- The use of a link, rather than an equivalent button, for the option to customise the end user's choice also makes this option far less salient.
- Amazon also uses language in the choice screens that is "non-neutral". For instance, there is no reference in the initial choice screen that this choice is about the combination or cross-use of personal data between separate Amazon services. Instead, the choice is presented as "Keep your Amazon services connected" and "staying connected" to be served "the most relevant experiences based on your interests across these services". End users will only see that the consent requested relates to the use of their personal data if they click on "Customise and learn more" or the "Data use between services" link in the last line of the screen.
- We also strongly question the use of a cookie banner to seek end users' consent to comply with the obligations in Article 5(2). Placing these important new choices required by the DMA in standard cookie banners likely leads to consumers closing them quickly without engaging with the choice to be made because consumers generally pay little attention to cookie banners.

5.3. Self-preferencing

Under Article 6(5), the Digital Markets Act prohibits gatekeepers from treating their own products and services more favourably than those of third parties. This means Amazon cannot self-preference its own services or products on its product search results page or in the Featured Offer, Second Offer, and All Offer Display Link on its product detail page.

Amazon says that its "ranking processes operate in an unbiased manner, using objective inputs and weighing them neutrally to facilitate the best possible customer choice irrespective of whether a product is offered by Amazon Retail or Sellers and therefore are in compliance with Article 6(5) of the DMA".

It would be important for Amazon to share data from the redesign of the Amazon product results page, including the Featured Offer, Second Offer, and All Offer Display Link on the product detail page with the Commission in order to assess compliance with Article 6(5).

5.4. Termination conditions

The DMA's Article 6(13) and related Recital 63 require Amazon to make the termination of its services possible without undue difficulty and that closing an account or unsubscribing should be as easy as opening an account or subscribing to the same service.

Amazon insists that its current processes enable customers, sellers, advertisers, and publishers to terminate the relevant services without undue difficulty but without providing evidence.

In 2022, Amazon was found, on the basis of a CPC complaint by BEUC's Norwegian member, Forbrukerrådet, BEUC and several other of its members, not to comply with consumer protection law with regard to the cancellation of Amazon Prime subscriptions. These cancellation practices consisted in a large number of hurdles to unsubscribe, including complicated navigation menus, skewed wording, confusing choices, and repeated nudging.

While subscribing to Amazon Prime is possible with two clicks, today this is still not the case for unsubscribing. On the basis of testing by BEUC on Amazon's website in several countries unsubscribing takes six or more clicks. This would appear to not be compliant with Article 6(13) and the related recital requirements. Amazon also continues to use behavioural techniques to try to discourage end users from unsubscribing which may subvert end users' free decision-making.

6. ByteDance

6.1. Inadequate compliance report

As set out above, the DMA (Article 11) requires gatekeepers to publish a non-confidential summary of their compliance report to enable third parties (including consumer representatives) to assess whether the gatekeepers comply with their obligations under the DMA. ByteDance does not follow the DMA requirements or the compliance template provided by the Commission. ByteDance does not include information on important issues for establishing compliance from the end user perspective, such as whether it tested its choice screens in relation to personal data use enable consumers to freely decide whether to consent to the use of their personal data. This undermines the effectiveness of its compliance report and does not fulfil the requirements of Article 11 DMA.

6.2. Use of consumers' personal data

The Digital Markets Act (Article 5(2)) restricts gatekeepers from using consumers' personal data for advertising purposes and combining/cross-using consumers' personal data from a gatekeeper's core platform service (for example, ByteDance's TikTok) with personal data

from another of their services or with personal data from third party services, unless the end user has freely consented to this.

Gatekeepers have to offer a choice which includes a less personalised but equivalent service if consumers do not wish to consent to the use of their data, and cannot make the use of the core platform service or certain of its functionalities conditional upon the end user's consent. The end user's choice must be freely given, specific, informed and unambiguous and cannot be undermined by behavioural techniques or user interface designs, including designs that are non-neutral, or that subvert end users' autonomy or decision-making on the use of their data (Article 13 anticircumvention clause).

ByteDance has said that TikTok already offers its end users a consent mechanism that complies with Article 5.2 requirements. However, the choice screens used by ByteDance raise doubts on its effective compliance with its DMA obligations under Article 5(2) in conjunction with Recitals 36 and 37, and Article 13, in particular Article 13(4) and Article 13(6). ByteDance's choice screens use "behavioural techniques or interface design" which exploit behavioural biases.

These include, for its choice screen on use of data for advertising (see Figure 8):

- ByteDance does not clearly explain the implications of the user's choice in this choice screen. It uses positive wording ("relevant ads", "personalized ads") to describe the option to accept data sharing for targeted ads. Rather than explaining that the second (Generic ads) option is not based on the user's personal data from multiple sources, ByteDance only states that "The ads you'll be shown may be less relevant to you". It is questionable whether this choice enables the end user to make a "freely given, specific, informed and unambiguous" choice on the use of their personal data as required.
- The use of the phrase "Allow us to use your data to show you relevant ads, which helps keep TikTok free" is misleading and likely encourages users to accept the use of their personal data for ads, in the absence of a clear explanation of the alternatives.

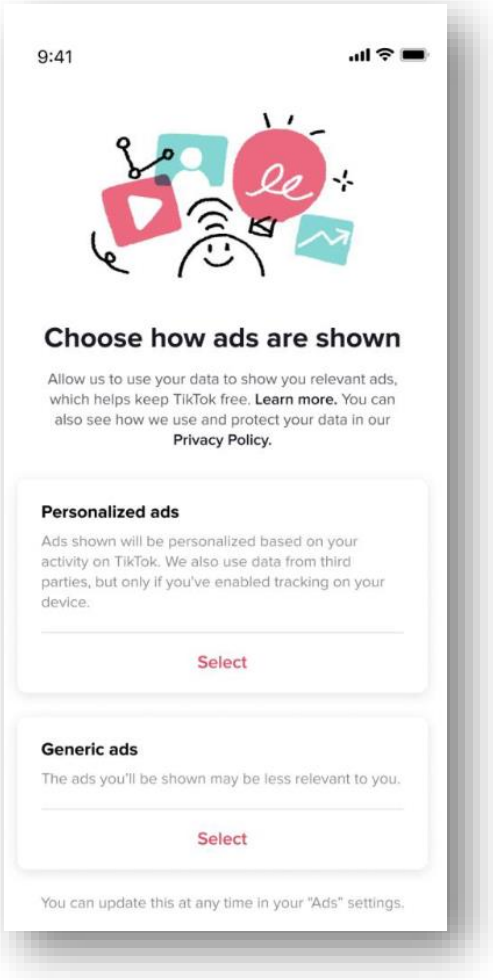

Figure 8: Screenshot for consent to personalised ads on TikTok

Regarding ByteDance's choice screen for the use of data between TikTok and other ByteDance services (CapCut), its use of behavioural techniques or interface design raise further non-compliance concerns (see Figure 9) including:

- The colours of the buttons to give or refuse consent are "non-neutral", and can "materially distort or impair the ability of end users to freely give consent", or "subvert end users' autonomy". The button to give consent is bright red whereas the option button to refuse it is transparent.
- ByteDance uses language in the choice screen that is unclear, misleading and "non-neutral" and can undermine the end user's ability to make a "freely given, specific, informed and unambiguous" choice. For example, there is no mention that this consent concerns personal data sharing, only that the end user is being asked if CapCut can "access"/ "read" certain information.

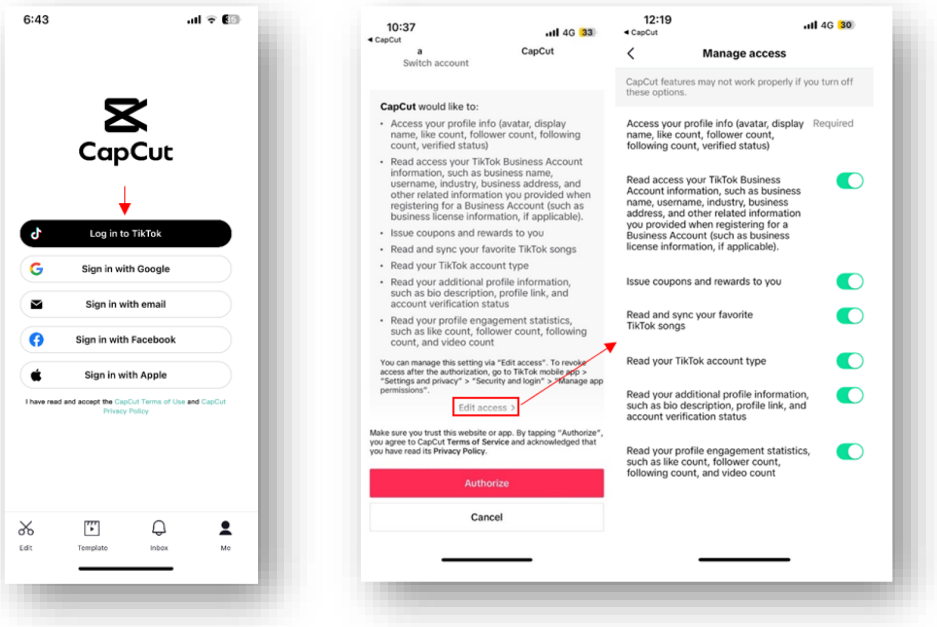

Figure 9: CapCut sign-in and data sharing consent flow

7. Microsoft

Use of consumers' personal data

The Digital Markets Act (Article 5(2)) restricts gatekeepers from using consumers' personal data for advertising purposes and combining/cross-using consumers' personal data from a gatekeeper's core platform service (for example, Windows) with personal data from another of their services or with personal data from third party services, unless the end user has freely consented to this.

Gatekeepers have to offer a choice which includes a less personalised but equivalent service if consumers do not wish to consent to the use of their data, and cannot make the use of the core platform service or certain of its functionalities conditional upon the end user's consent. The end user's choice must be freely given, specific, informed and unambiguous and cannot be undermined by behavioural techniques or user interface designs, including designs that are non-neutral, or that subvert end users' autonomy or decision-making on the use of their data (Article 13 anticircumvention clause).

Microsoft does not appear to obtain "freely given", "specific", "informed" and "unambiguous" consent choices from consumers when asking them about combining their data from Windows with data from other services in accordance with Article 5(2) and Article 13 in several cases.

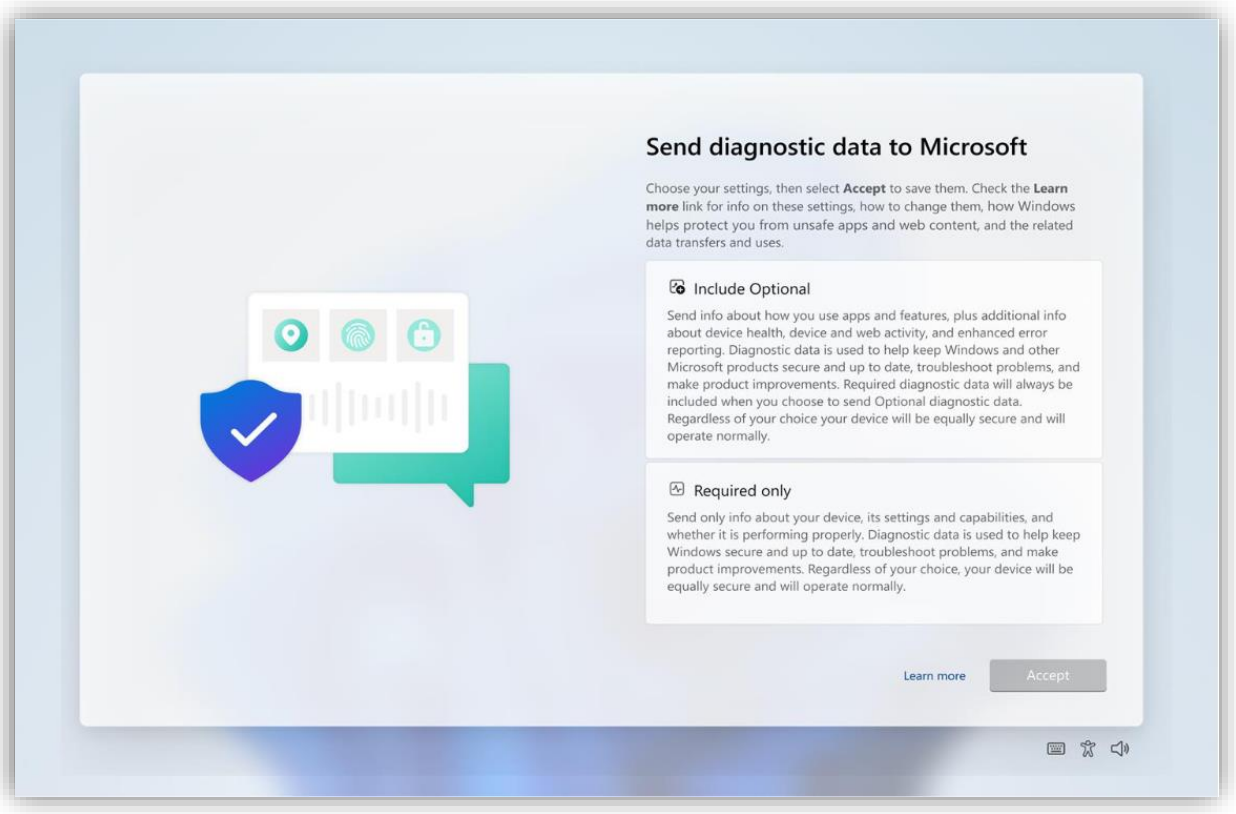

Figure 10: Windows consent to collect optional diagnostic data in the device setup experience

Figure 10 shows the choice screen Windows presents to end users to collect and use optional diagnostic data during the device setup experience. This is an example of several choice screens that Microsoft provides to end users which raise doubts about effective compliance. Concerns include:

- Microsoft not specifying which of its products the data is shared with beyond "Windows and other Microsoft products." This does not enable consumers to make an informed choice.
- Using vague terms such as 'info' and 'diagnostic data' is likely to mislead consumers because there is no mention of their personal data being used.

Microsoft's LinkedIn choice screens also raise concerns under Articles 5(2) and 13 relating to the use of data for advertising or on combination and cross-use of data.

For instance, Microsoft seeks consent for its LinkedIn Marketing Service (LMS) to target ads to LinkedIn members based on third-party data received from LMS advertisers. This choice screen is shown below in Figure 11.

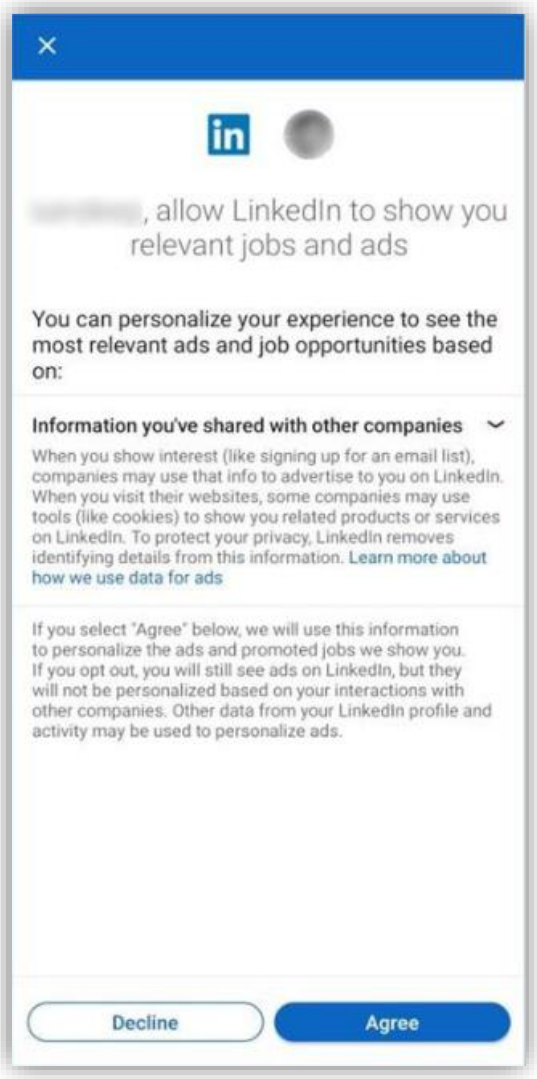

Figure 11: Consent screen for LinkedIn advertising data

However:

- The colours of buttons to agree or decline are "non-neutral". The button to consent is blue while the button to decline is white. This behavioural technique can exploit end users' 'saliency bias', thereby visually steering the end user to consent to personal data use.
- LinkedIn does not use the term "personal data" but "info" or "information".
- Microsoft also bundles two separate services together when it asks for consent to the personalisation of its ads and the jobs it promotes to users. This bundling puts users at a disadvantage if they do not want their data to be used for targeted ads but do seek promoted jobs. Microsoft appears to be exploiting the likely interest of users in its promoted jobs section to obtain their consent for targeted ads. This is unlikely to lead to "specific", and "unambiguous" consent.

8. Importance of testing end user interfaces and documentation on design choices

To demonstrate compliance with the DMA as is required (Article 8), it is essential for gatekeepers to test each of their end user interface designs on actual consumers in relation to the terms of the relevant DMA obligation and the DMA's anticircumvention provision prior to the roll-out of the user interfaces to make sure that consumers understand the choice that they are being asked to make and to ensure that their choices are freely given, specific, informed and unambiguous. The user interface designs should also be subject to prior consultation. The testing results and data on the choices made by end users following roll-out must be provided to the Commission and relevant third parties for analysis of compliance.

The Commission, in exercise of its powers under the DMA, should also require gatekeepers to provide as all their internal records explaining their choice of user interface designs.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.