BEUC The European Consumer Organisation

The European Consumer Voice

Cosmetic compliance

How the gatekeepers continue to undermine compliance with the Digital Markets Act 2025-26

November 2026

The European Consumer Organisation (BEUC) is the largest organisation promoting the general interests of Europe's consumers. Founded in 1962, it proudly represents more than 42 independent national consumer organisations from over 31 European countries. Together with our members, we inform EU policies to improve people's lives in a sustainable and fair economy and society.

BEUC, The European Consumer Organisation
Bureau Européen des Unions de Consommateurs, AISBL | Der Europäische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.beuc.eu
Enterprise No.: BE 0422 071 051• EC register for interest representatives: identification number 9505781573-45

Rue d'Arlon 80,
B-1040 Bruxelles
Tel : +32 (0)2 743 15 90
www.beuc.eu
Contact: competition@beuc.eu

BEUC-X-2026-101
November 2026

Co-funded by
the European Union

Views and opinions expressed do not necessarily reflect those of the European Union or EISMEA 2026. Neither the European Union nor the granting authority can be held responsible for them.

Contents

Why it matters to consumers 5

About this report 5

Our call to the Commission 6

A lack of effective compliance 6

Action on circumvention 6

Monopoly of enforcement and effective remedies 6

Key findings 7

In a nutshell 7

Per gatekeeper 9

Alphabet 9

Consent for use of personal data 9

Steering 9

Tying 9

Uninstalling and setting alternative apps as defaults 9

Alternative app stores and sideloading 10

Self-preferencing 10

Amazon 10

Consent for use of personal data 10

Price controls 11

Apple 11

Steering 11

Alternative app stores and sideloading 11

Interoperability with the gatekeeper's operating system 12

ByteDance 12

Consent for use of personal data 12

Termination of service 12

Meta 12

Consent for use of personal data 12

Tying 13

Termination of service 13

Microsoft 13

Consent for use of personal data 13

Uninstalling and setting alternative apps as defaults 13

ANNEX

Detailed findings per gatekeeper 14

1. Alphabet 15

1.1 Consent for use of personal data 15

Combining first and third-party sources of personal data for ads 15

Cross-use/combination of personal data across different services 17

1.2. Steering 18

1.3. Tying 18

1.4. Uninstalling and setting alternative apps as defaults 21

1.5. Alternative app stores and sideloading 25

1.6. Self-preferencing 27

2. Amazon 29

2.1. Consent for use of personal data 29

2.2. Price controls 31

3. Apple 33

3.1. Steering 33

3.2. Alternative app stores and sideloading 35

3.3. Interoperability with the gatekeeper's operating system 38

4. ByteDance 39

4.1. Consent for use of personal data 39

4.2. Termination of service 43

5. Meta 46

5.1. Consent for use of personal data 46

Combining first and third-party sources of personal data for ads 46

Cross-use/combination of personal data across different services 48

5.2. Tying 52

5.3. Termination of service 53

6. Microsoft 58

6.1. Consent for use of personal data 58

6.2. Uninstalling and setting alternative apps as defaults 61

Why it matters to consumers

The Digital Markets Act (DMA) aims to **stop tech giants from abusing the enormous power of their core platform services** to harm consumers and other users and to create a **fairer digital economy.**

The DMA does this by setting rules from the get go for gatekeepers to ensure digital markets are fair and contestable. This includes pre-empting harmful conduct before it happens and opening up platform services to more innovation and choice, rather than trying to sanction companies using competition law once the damage has been done.

For consumers, this approach is likely to yield substantial benefits **if gatekeepers effectively comply with it and, where needed, the Commission enforces it fully and vigorously**. By nipping illegal conduct in the bud, it could give consumers greater choice in terms of services, prices and innovation.

For example, the DMA enables consumers to install on their devices, and set as default, **different alternative app stores, apps, browsers, search engines or payment systems** than those of the gatekeepers. It also gives them greater choice regarding what happens to their **personal data** and creates the possibility for devices from different manufacturers to **interact** with one another.

About this report

The European Consumer Organisation (BEUC) has been closely monitoring **gatekeeper compliance** with the Digital Markets Act. We have been drawing attention to potentially non-compliant behaviour by the gatekeepers since March 2024 with over 21 submissions made to the Commission.[1]

This report summarises some of the material already submitted to the Commission from June 2025 until June 2026. It contains both a key findings section and a more detailed findings section.

This report **is not an exhaustive list of all non-compliant behaviour** under the DMA, nor does it cover all the DMA's provisions. It reflects the areas where BEUC has assessed gatekeeper compliance proposals for itself through in-house testing and through publicly available information, such as the gatekeeper compliance reports. It reflects areas where consumers directly interact with gatekeeper interfaces. It relies largely, but not solely, on behavioural analyses of the user interfaces gatekeepers have put in place.



1 BEUC has summarised its findings so far in 2 reports: BEUC, *Implementation by Meta, Apple, Google, Amazon, Bytedance and Microsoft of their obligations under the DMA* (2 Sept. 2024, accessed 13 Oct. 2026); and BEUC, *November 2024 update on implementation by Apple, Google & Meta of their obligations under the DMA - BEUC analysis of non-compliance* (13 Nov. 2024, accessed on 13 Oct. 2026). BEUC has also published a report into the benefits that have already emerged for consumers from the DMA: BEUC, *First bloom: increased consumer choice after eighteen months of the DMA* (5 Nov. 2025, accessed on 13 Oct. 2026).

Our call to the Commission

A lack of effective compliance

The DMA relies heavily on the concept of '**effective compliance.**' This means that gatekeepers should not only comply with the DMA's individual obligations on paper but also that the measures they put in place **comply in their effectiveness**.

BEUC calls on the European Commission to **accelerate its enforcement of the DMA**, due to the lack of effective compliance by the gatekeepers with many of their obligations two-and-a-half years into the application of the DMA. The Commission needs to **fully and vigorously enforce** the DMA's provisions**,** if necessary through stronger sanctions of the gatekeepers.

Contrary to what several gatekeepers claim in compliance reports, BEUC believes that their compliance is at times **selective and partial**, undermined by the use of various **behavioural techniques** and **non-neutral interfaces**. In some cases, DMA breaches can take a more **overt, openly defiant approach**. For example **Alphabet** on self-preferencing, **Apple** on steering, or **Meta** on personalised ads, each of which will ultimately be resolved after years of litigation before the European Courts. Such a course of action deprives consumers of greater choice and digital markets of fairness and contestability that the DMA is supposed to provide.

Action on circumvention

BEUC calls on the Commission to urgently address gatekeepers' compliance with **Article 13** of the DMA, which **prohibits circumvention** and which has, to date, not been enforced.

Article 13 is a **fundamental** part of the DMA. It allows the regulator to specifically **prevent behavioural techniques, interface designs and non-neutral information** which can have the effect of undermining compliance with individual obligations.

BEUC highlights throughout this report examples of the gatekeepers using various techniques that likely **sway consumers to take decisions which they would not have done had gatekeepers presented choices in a fairer and more neutral manner**.

The European Commission must more **pro-actively scrutinise changes, interfaces and user flows** put in place by gatekeepers to ensure they meet the **key criterion of effectiveness** that the DMA requires.

Monopoly of enforcement and effective remedies

Finally, in some of the DMA investigations which led to non-compliance decisions, we are concerned that the Commission appears to be hesitant to pursue **all forms of gatekeeper circumvention.**

This is the case in both the Meta investigation, on pay-or-consent[2] , and in the twin Apple investigations, on steering[3] and alternative distribution.[4] In the first case, Meta for example continues to offer a **degraded experience** to users such as forced ad breaks if they select the 'less personalised ads' option. Meta uses **non-neutral interfaces and behavioural techniques** including **delaying the third option in the user flow**, and prevents users from **providing consent as required under the General Data Protection Regulation (GDPR)**. In the Apple cases, Apple appears to continue to use **non-neutral information** in its interfaces and imposes **substantial fees** for steering and alternative distribution.

For the DMA to succeed, the outcome of these investigations must lead to **new and better choices for both business users and end users**. The Commission therefore holds a special responsibility, as the DMA's sole enforcer, to extract **effective remedies** from reluctant gatekeepers.

---

2 Case DMA.100055
3 Case DMA.100109
4 Case DMA.100206

To achieve that goal, **the Commission needs to more systematically seek input from relevant third parties such as consumer groups, on possible remedies and the commitments made by gatekeepers. Because of their daily work, consumer groups can assess** the impact of gatekeeper proposals on users' decision-making and behaviour. This is essential to ensure that the benefits of the DMA materialise for consumers.

Key findings

In a nutshell

Between 2025 and 2026, BEUC has found substantial evidence indicating that most of the gatekeepers - Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft - continue to **comply only selectively with the Digital Markets Act** (DMA).

Two broad trends appear.

First, most of the gatekeepers frequently use **behavioural techniques and non-neutral interfaces when interacting with consumers,** undermining their compliance with the substantive provisions of the DMA. This is despite the DMA having a clear prohibition on the use of non-neutral interfaces, and of behavioural techniques if they undermine effective compliance. The use of these techniques and interfaces is very likely to have a detrimental effect on the ability of consumers to enjoy the full benefits of the DMA.

Second, various gatekeepers continue to **limit and stall** their full compliance with the DMA provisions that **go to the heart of their business models.** This is the case for:

- **Meta on seeking consent to use personal data;**
- **Apple on steering, interoperability or allowing alternative app distribution;**
- **Alphabet on seeking consent for use of personal data, self-preferencing, steering, allowing alternative app distribution, default choices;**
- **Amazon on price controls.**

The table and section below summarise areas where BEUC has detected non-compliance with the DMA. A more detailed set of findings, including screenshots, is available in the annex, which contains more detailed findings.

	Consent for personal data use	Allow steering	Stop tying	Allow uninstallation of gatekeeper apps and changing defaults	Allow installation of alternative apps and app stores through alternative distribution	No self-preferencing
Alphabet	X	X	X	X	X	X

	Consent for personal data use	Parity clause or equivalents
Amazon	X	X

	Allow steering	Allow installation of alternative apps and app stores through alternative distribution	Interoperability
Apple	X	X	X

	Consent for personal data use	Termination of service
Byte Dance	X	X

	Consent for personal data use	Stop tying	Termination of service
Meta	X	X	X

	Consent for personal data use	Allow uninstallation of gatekeeper apps and changing defaults
Microsoft	X	X

Per gatekeeper

Alphabet

Consent for use of personal data

Alphabet continues to use **non-neutral language** in its various consent screens to **cross-use or combine users' personal data** across its different services. Non-neutral elements should be identified, removed and replaced with more neutral texts/interfaces. Their use is illegal and is likely to steer consumers to make choices that they would not otherwise make.

Alphabet also relies on the Interactive Advertising Bureau'sTransparency and Consent Framework (TCF) to obtain consent for ad purposes under the DMA. This is problematic as TCF consent banners fail to clearly and explicitly inform the user that, in consenting, they are consenting to Alphabet's combination of their data from this third-party source with data generated on services belonging to Alphabet for personalised ads purposes, which the DMA requires.

(For more details, see Section 1.1 of the annex, pp 15-17)

Steering

The Commission already imposed a Non-Compliance Decision[5] on Alphabet in July 2026 for failing to respect the DMA obligation to allow steering. Alphabet had 60 days from that date to propose compliant changes, but it is too early to tell if Alphabet is now compliant or not. BEUC has not seen any new proposals from Alphabet.

Prior to the Non-Compliance Decision, BEUC's concerns related to the **overlapping and extensive fees** Alphabet was charging app developers for steering and the potential **non-neutrality of the information screen** that Alphabet required app developers to display every time they were steering a consumer outside the app environment. BEUC also expressed concerns about the **level of discretion** Alphabet has in denying or revoking access to the External Offers Program[6], in which participation is essential to be able to engage in steering.

(For more details, see Section 1.2 of the annex, p 18)

Tying

Alphabet continues to use **several interface design and behavioural techniques** to undermine its compliance with the **ban on tying**. While the gatekeeper now allows using third-party email addresses to create a Google Account, it still makes **Gmail options disproportionately prominent** over third-party email options for both adult and child accounts. For example, Alphabet provides ready-made, available choices of Gmail addresses, or has Gmail pre-selected as the domain name in a box, in the process to decide which email address to use for a Google Account. Options to use Gmail for a child Google Account are more numerous, more salient and less demanding in terms of time and effort, than the choice to use a third-party email address.

(For more details, see Section 1.3 of the annex, pp 18-20)

Uninstalling and setting alternative apps as defaults

Alphabet continues to undermine consumers' ability to easily change default settings or to uninstall gatekeeper apps. For instance, Alphabet prevents Pixel devices users from **uninstalling Google Search, Chrome, the Play Store, Google Maps or YouTube**. Alphabet also displays **'scare screens'** to dissuade users from disabling one of these apps (disabling is still not the same as uninstalling)

Certain **features on Pixel devices** continue to **steer** usersconsumers to Alphabet products even after they select an alternative third party service. This includes features such as the Circle-to-Search feature at the bottom of a Pixel device which leads to Google Search, or the fact that Chrome remains in the dock even after the user has selected

5 European Commission, *Commission fines Google €890 million for breaches of the Digital Markets Act* (23 July 2026, accessed 25 Sept 2026).

6 Google Console Play Help, *Developer Terms Of Service For External Offers Program* (published date unknown, accessed on 17 October 2025).

an alternative browser as their default. Gmail also has a feature, which is on by default, to open links in Gmail rather than the default browser.

Finally, Alphabet continues to regularly display **prompts** to users to switch to its apps after a third-party app has been selected as the default. It is difficult to say how often such prompts appear, but what is clear is that their repeated use may undermine users' ability to easily change their default settings, as the DMA requires. Commission guidelines or specifications laying out what types of prompts, and how often they can be displayed, would be useful.

(For more details, see Section 1.4 of the annex, pp 21-25)

Alternative app stores and sideloading

Alphabet has introduced **unnecessary hurdles and non-neutral elements** in the process to download an alternative app store. These practices create negative friction for users, which may dissuade them from continuing the process and thus may breach the DMA. For instance, the default setting on a Pixel device is not to allow the download of a third-party app store, requiring a manual change of the settings to reverse it, despite such downloads being expressly allowed under the DMA.

Alphabet also uses scare screens, non-neutral interfaces and behavioural techniques when the user does attempt to install a third-party app store. The screens displayed use alarmist language highlighting security risks of using third-party app stores, which are likely to have a dissuasive effect on users. Finally, there is no setting on a Pixel device allowing the user to select a third-party app store as the default app store.

(For more details, see Section 1.5 of the annex, pp 25-27)

Self-preferencing

Alphabet has already **fallen foul** of the DMA's self-preferencing prohibition, as underlined by a Commission Non-Compliance Decision[7] issued on 23 July 2026. Alphabet had 60 days from that date to enter into compliance, yet it is clear to BEUC that Alphabet continues to engage in self-preferencing in its Google Search results pages.

First, regarding shopping services, Alphabet continues to give greater prominence to its **product ads unit** (*"Sponsored products"*) compared to any similar comparison-shopping service belonging to third parties.

Second, Alphabet appears to **systematically display its own comparison service in the products unit** of Google Search whether for hotels, shopping, flights or any other service addressed in the decision. However, Alphabet does not grant the same degree of visibility to individual third parties, given that only a handful are displayed at a time in the accordion. For shopping services at least, Alphabet regularly only displays its own service in the *"Comparison Sites"* unit.

Third, Alphabet continues to display results for product units using **Google Maps** on Google Search rather than also allowing the display of alternative maps services.

Finally, Alphabet continues to display its own **translation or sports services** prominently at the top of the Google Search results pages, depriving rival third-party services from achieving the same level of prominence.

(For more details, see Section 1.6 of the annex, pp 27-28)

Amazon

Consent for use of personal data

Amazon continues to use **behavioural techniques and interface designs** which undermine its effective compliance with the DMA when obtaining consent before **using or combining users' personal data** across different services. Amazon systematically frames in a positive way the option to consent to the cross-use/combination of the user's personal data, which is neither balanced nor objective. The texts also use vague terms and use brightly coloured buttons to make the 'consent' option more salient.

(For more details, see Section 2.1 of the annex, pp 29-30)

7 European Commission, *Commission fines Google €890 million for breaches of the Digital Markets Act* (23 July 2026, accessed on 12 June 2026).

Price controls

Although Amazon no longer appears to use so-called 'parity clauses' in its terms with third-party sellers, BEUC is concerned that **Amazon's price controls have an equivalent effect** and breach the DMA.

These price controls affect the visibility of products on sale on Amazon if they are simultaneously on sale on a third-party marketplace at cheaper prices. The limits that Amazon imposes on such products range from no longer being displayed as a Featured Offer or Second Displayed Offer on Amazon to being delisted on the platform altogether. These unilateral price controls imposed by Amazon are likely to have a chilling effect on sellers who want to sell both on Amazon and a cheaper marketplace.

(For more details, see Section 2.2 of the annex, pp 31-32)

Apple

Steering

The Commission has already imposed a Non-Compliance Decision on Apple in April 2025 for failing to respect the obligation to allow steering.

Apple announced new terms on 18 August 2026[8] which became operational from 1 October 2026. However, BEUC is concerned that **the new terms do not resolve fundamental non-compliance issues.**

For instance, the disclosure sheet Apple requires developers to display when they steer users outside the app environment still appears to use **behavioural techniques** and **non-neutral language** which may undermine Apple's compliance. The fees Apple intends to charge for steering also raise questions. First, it is unclear how Apple is able to **charge for the act of steering**, as Apple puts it, rather than for the "*initial acquisition*" which the DMA allows. Second, the reaction of game and major app developers, who do not appear to want to use this channel if it is associated with such fees, raises doubts as to whether consumers will benefit from the new steering possibilities created by the DMA.

(For more details, see Section 3.1 of the annex, pp 33-34)

Alternative app stores and sideloading

The Commission published preliminary findings of non-compliance in April 2025 against Apple for not enabling alternative app store and app distribution.[9] Under the same deal mentioned in the previous sub-section, Apple put forward new terms for the installation of apps and app stores through alternative channels. BEUC has two main concerns: fees and user experience.

First, **Apple's 5% commission** on the sale of any digital goods or services provided through an app that has been installed from an alternative app store or from the web appears to be high. BEUC is concerned at the possibility that such a fee **will limit possibilities for alternative app stores** to operate in an iOS environment.

Second, while Apple has released only some of the new user flows for the installation of alternative apps and app stores,[10] these user flows still contain **negative friction points** such as behavioural techniques and excessive number of steps, which may deter users from completing the installation process.

(For more details, see Section 3.2 of the annex, pp 35-37)

8 Apple, *Apple announces changes for apps in the European Union* (18 August 2026, accessed 26 August 2026).
9 European Commission, *Commission closes investigation into Apple's user choice obligations and issues preliminary findings on rules for alternative apps under the Digital Markets Act* (23 April 2025, accessed 20 Oct. 2026).
10 Apple, *Alternative distribution installation experience updates* (date unknown, accessed on 26 August 2026).

Interoperability with the gatekeeper's operating system

Apple's first attempts to comply were **deemed insufficient** both by the Commission and various third-party business users. As a result, the Commission recently published two sets of specifications to clarify how Apple needed to comply with this provision.

Apple has yet to show whether it will comply.

(For more details, see Section 3.3 of the annex, p. 38)

ByteDance

Consent for use of personal data

ByteDance consistently uses **non-neutral language and behavioural techniques** throughout its consent screens to use/combine personal data across different services. For example, ByteDance consistently frames the option to provide consent in a positive way, while only highlighting negative points if the user declines. In addition, the information ByteDance provides to users is inadequate to make an informed decision as both the DMA and GDPR require. Revoking consent is also considerably harder than providing it, with ByteDance forcing users to go through eight steps to complete the revocation of consent.

(For more details, see Section 4.1 of the annex, pp 39-42)

Termination of service

ByteDance's procedure for closing a TikTok account involves **9 screens and 11 steps**, which is far more complex and burdensome than the process to open an account is. BEUC considers this to be a breach of the provision on termination of service.

(For more details, see Section 4.2 of the annex, pp 43-45)

Meta

Consent for use of personal data

Meta was already found non-compliant by the Commission in April 2025 with its binary 'pay-or-consent' choice for ad purposes,[11] which it introduced ahead of the entry into application of the DMA. Meta's latest changes, rolled out in January 2026, have however not solved its compliance issues with the DMA, GDPR or consumer law, in BEUC's opinion. BEUC has already carried out an analysis[12] about why Meta's user flow may still be breaking the law.

Meta continues to **use non-neutral language and interface design techniques** in its user flow, **undermining the free choice of users** under the DMA. For instance, Meta continues to provide the **less personalised ads choice later in the user flow** and with a **degraded user experience because of ad breaks**. Meta also prevents users from providing free, specific, informed and unambiguous consent as required under the GDPR.

Separately, Meta needs to seek consent to use/combine a consumer's personal data across its different services. For each of the interfaces however, Meta uses **non-neutral information, behavioural and interface design techniques to steer users to consent**, undermining Meta's effective compliance. For instance, by first enabling the cross-use/combination of personal data across different services and then seeking user consent to keep the services linked, Meta is using 'status quo bias' to its advantage knowing that users are more likely to stick to default settings, especially if the alternative requires more effort.

(For more details, see Section 5.1 of the annex, pp 46-52)

---

11 European Commission, Commission finds Apple and Meta in breach of the Digital Markets Act (23 April 2025, accessed 14 October 2026).

12 BEUC, Report: 'Users Still Stuck in the Mud: An Analysis of Meta's 2026 Changes to its Consent-for-Ads Mechanism against EU Law' (17 March 2026, accessed on 7 September 2026).

Tying

BEUC is concerned that the way Meta has designed the setup of a Facebook account effectively constitutes tying which is in breach of the DMA.

When end users create a Facebook account for the first time, at no point during the account creation process do they receive a **choice about whether they want to use Messenger within Facebook**. This is despite Messenger being designated as a separate core platform service from Facebook under the DMA. It is only after setup and use of the Facebook account that Meta prompts end users to decide whether they want to continue using Facebook and Messenger together or to separate them. However, the design of the account creation process in this manner plays on **status quo bias** and limits the likelihood that users will separate Messenger from Facebook. A **clearer separation** of the two services may be necessary.

(For more details, see Section 5.2 of the annex, pp 52-53)

Termination of service

Meta makes the termination of either Facebook or Instagram **considerably more difficult** than the creation of the account and thus breaches the DMA, in BEUC's opinion.

Unsubscribing from either Facebook or Instagram is a **non-intuitive and unnecessarily long sequence of steps.** There are sixteen steps in total, which is considerably longer than the steps necessary to create an account.

(For more details, see Section 5.3 of the annex, pp 53-57)

Microsoft

Consent for use of personal data

Microsoft uses **behavioural techniques** and **non-neutral interfaces** in many of its choice screens to obtain consent from users to combine or use their data across different services.

For example, Microsoft consistently frames the use/combination of personal data across services in very positive terms, emphasising various benefits, while there are no explanations as to why the user may want to decline. Microsoft also uses **behavioural techniques** like leaning on status quo bias or loss aversion bias to try to influence what users choose, which undermines the gatekeeper's effective compliance.

One noteworthy exception, however, is LinkedIn's choice screen seeking consent for ads purposes. It does not use any obvious non-neutral language, interface design or behavioural techniques, and other gatekeepers could find inspiration in this type of interface.

(For more details, see Section 6.1 of the annex, pp 58-61)

Uninstalling and setting alternative apps as defaults

Microsoft engages in conduct which **undermines the ability of end users to easily change their default settings** on Windows.

For instance, default links from Microsoft apps continue to open in Edge even after an alternative browser has been set as default unless Edge is uninstalled or the user expressly sets links from that specific app to open in their default browser. Microsoft also continues to unfairly favour Bing as a search engine in certain scenarios, for example when using Windows Search. The absence of an option to set a search engine as default across Windows makes it easier for Microsoft to steer end users to Bing in certain conditions.

Microsoft also regularly prompts users who have selected an alternative browser or search engine to switch to Edge or Bing using increasingly subliminal techniques, such as prompts coming from the device manufacturer, which undermine effective compliance with the DMA.

(For more details, see Section 6.2 of the annex, pp 61-63)

ANNEX

Detailed findings per gatekeeper

1. Alphabet

1.1 Consent for use of personal data

The DMA's Article 5(2) requires gatekeepers to seek consent from consumers before:

1. Combining their personal data from first and third-party sources for ads purposes;
2. Combining their personal data from the gatekeeper's core platform service with any other service;
3. Using their personal data from the gatekeeper's core platform service in another service provided by the gatekeeper;
4. Signing them in to other gatekeeper services to combine their personal data.

The DMA's recitals lay out further conditions, while Article 13 DMA prevents circumvention and consent must meet the criteria laid out in the GDPR.

BEUC is concerned that Alphabet might **not meet these obligations** on several points.

Combining first and third-party sources of personal data for ads

Alphabet says that it "*relies on its third-party consent framework (the "EU user consent policy"). Under this framework, Google requires advertising partners to obtain legally valid end user consent on their own service corresponding to their use of cookies or other local storage, and their collection and sharing of end user personal data for the personalization of ads. Under this framework, Google has requirements for advertising partners to send Google affirmative signals representing such users' consent statuses.*"[13]

BEUC questions the continued use of the **Interactive Advertising Bureau (IAB)'s Transparency and Consent Framework (TCF)** to obtain consent for DMA purposes in the past. Beyond the fact that the IAB's TCF framework has been heavily criticised by data protection authorities in the past, and is already subject to ongoing investigations under EU data protection law, cookie banners on third-party websites are generally not sufficiently explicit in seeking the particular consent Alphabet requires for DMA purposes.

These TCF cookie banners seek consent for the use of personal data often by **hundreds of third parties at the same time as Alphabet**, and for **many different purposes**. A cursory look at examples of such cookie banners shows that the specific consent that Alphabet seeks for DMA purposes is **virtually inconspicuous**.

For example, the cookie banner on a well-known French sports website (see figure 1 and 2) does not mention Alphabet/Google once in the top-level screen, let alone the specific purpose for which consent is required under the DMA. It is only by digging several levels down, which will be imperceptible to most consumers, that the cookie banner appears to seek consent for the relevant DMA purpose, though even this is not fully clear. Such an interface on countless third-party websites appears to be the only means by which Alphabet seeks consent for combining first and third-party sources of personal data for its ads service, as there is no secondary layer on Alphabet services seeking consent for the combination of first and third-party sources of personal data for ad purposes.

Such a framework is unlikely to **meet requirements for consent under the DMA**, as the consumer is unlikely to realise they are consenting to Alphabet's combination of their data from this third-party source with data generated on services belonging to Alphabet for personalised ads purposes through such a cookie banner. BEUC argues that the consumer is therefore unable to provide specific, informed, freely given consent for this specific purpose of personal data combination, as the GDPR and DMA require. BEUC urges the Commission to investigate Alphabet's compliance with Article 5(2) on this point.

13 Alphabet, *EU Digital Markets Act (EU DMA) Compliance Report Non-Confidential Summary* (6 March 2026, accessed 18 September 2026), page 9.

Figure 1: steps 1-2 of the TCF framework on a French sports website[14]

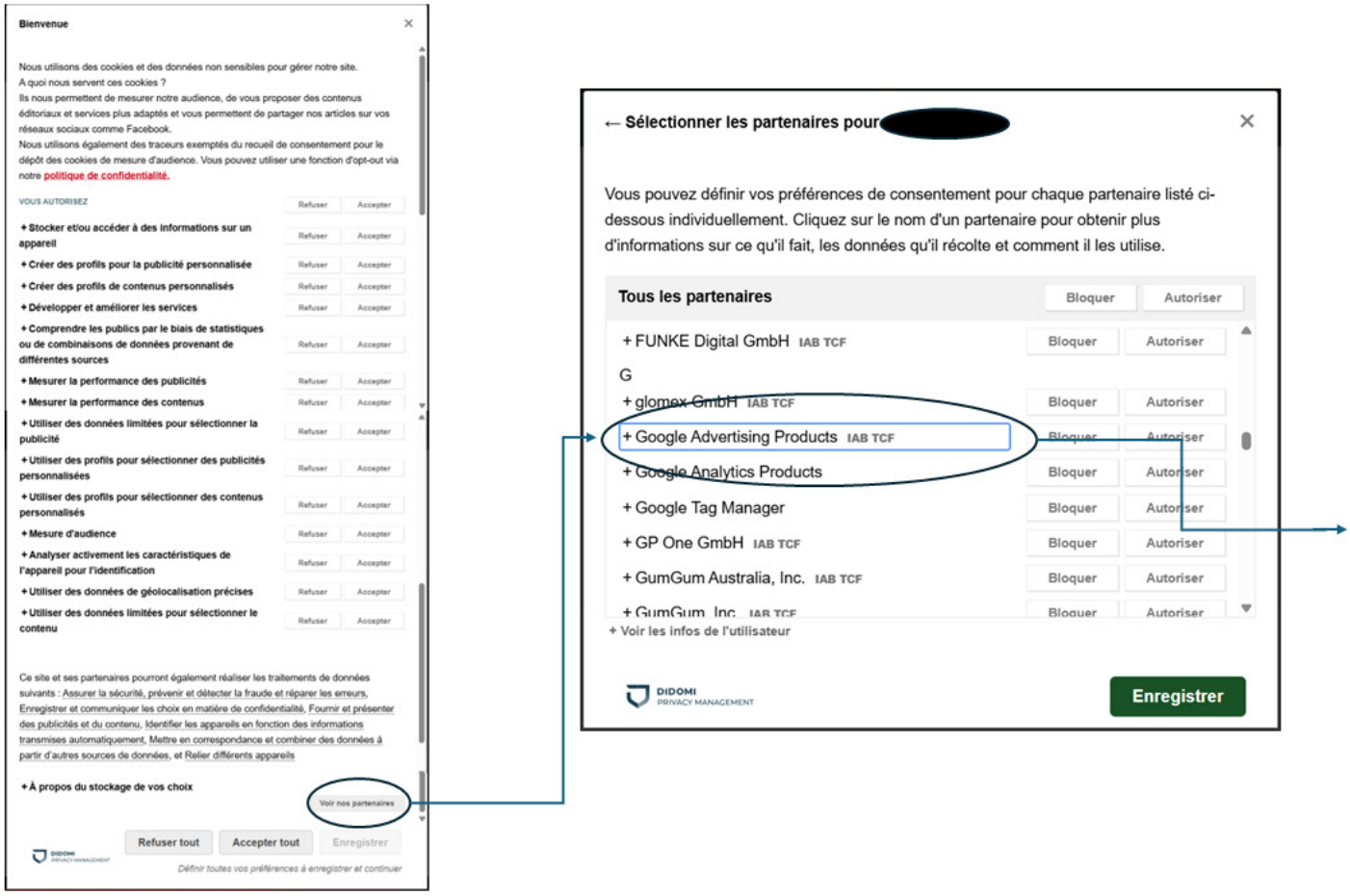
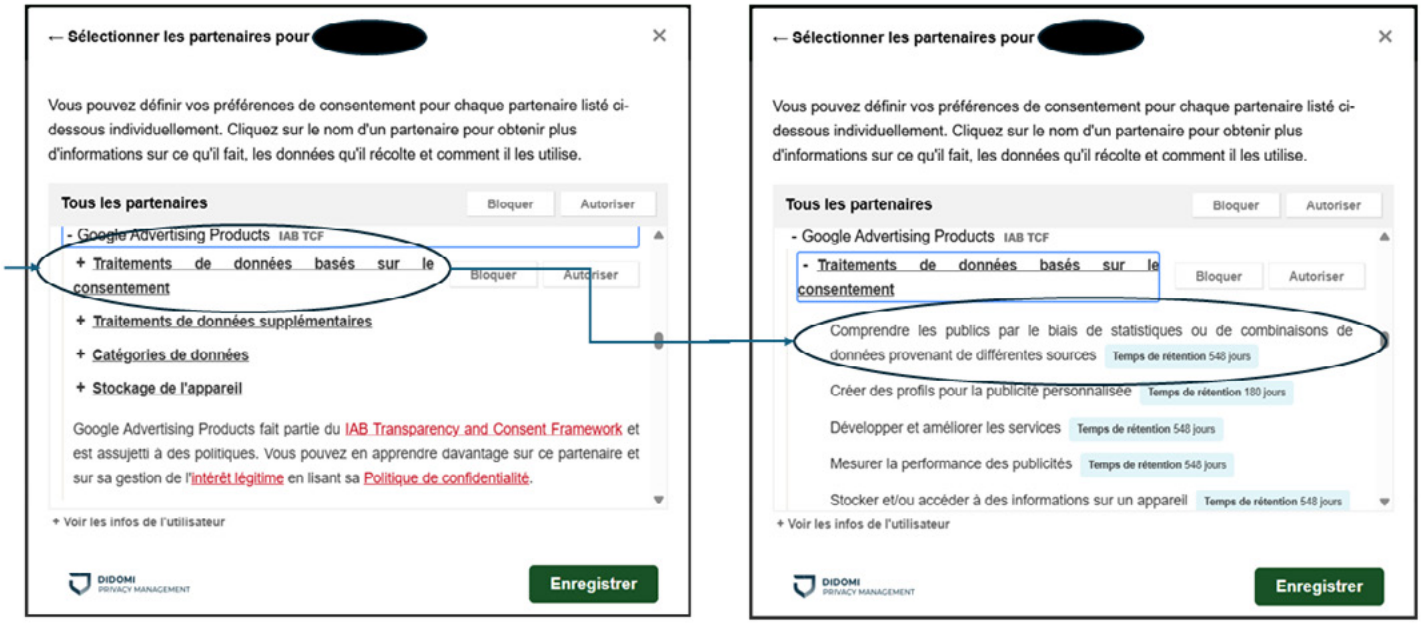


Figure 2: steps 3-4 of the TCF framework on a French sports website[15]



14 BEUC testing on French sports website on HP Windows device on 18 September 2026.
15 BEUC testing on French sports website on HP Windows device on 18 September 2026.

Cross-use/combination of personal data across different services

Alphabet uses **non-neutral language** in its user flows to **steer end users towards consenting to the cross-use or combination of their personal data** across different Alphabet services.

For example, in the interface seeking consent to use/combine the consumer's personal data from YouTube with data generated using other services (see figures 3a and 3b below), Alphabet presents reasons throughout the user interface as to why end users might want to link their services, but no information as to why users may want to decline their linking.

For instance, Alphabet says *"When linked these services can share data with each other and with all other linked Google services to: combine data to help personalize content and ads; develop and improve our services; measure and improve the delivery of ads."*

This description appears to be **neither balanced nor objective**, as it mentions only advantages to the user's personal data being cross-used/combined, and there is **no corresponding description for the option to decline**.

The effect of this is an **asymmetry of information** for users. In turn, users may be more likely to consent to the use/combination of their personal data across services, given that the information they receive suggests there are only benefits to link their data across the different services.

Alphabet's use of non-neutral elements in its interface **likely breaches Article 13 DMA** and **may also breach Article 5(2) DMA. Non-neutral elements should be identified, removed and replaced with more neutral texts/interfaces.**

BEUC is also concerned as to whether Alphabet has used/combined user personal data for the training of **Alphabet's AI foundation models or Gemini**. BEUC believes that Alphabet should seek consent from end users for these purposes **before** any data combinations takes place.

Figure 3a: user interface on YouTube for cross-use/combination of personal data across Alphabet's services[16]

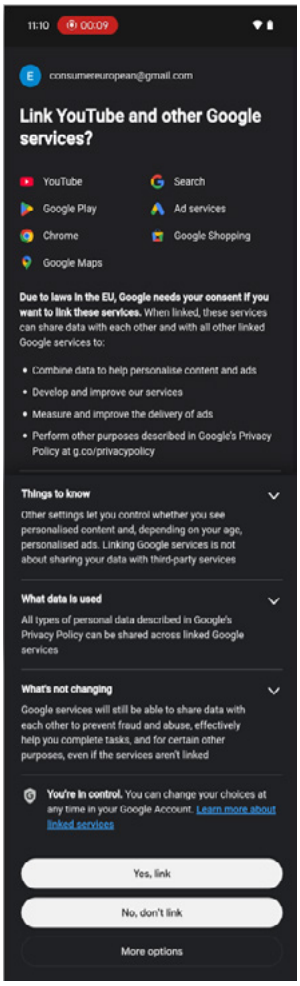
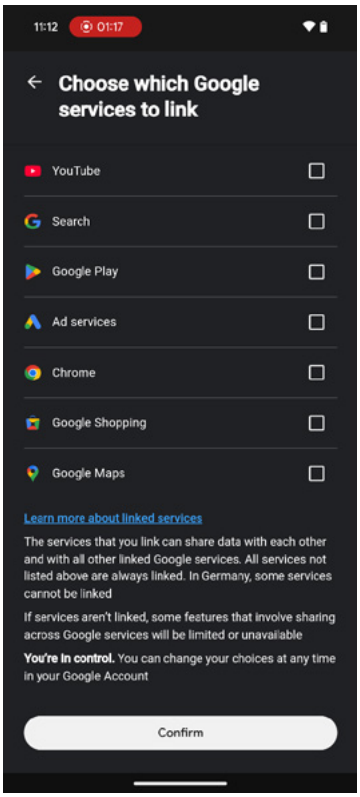


Figure 3b: clicking on "More options" on user interface on YouTube for cross-use/combination of personal data across Alphabet's services[17]



16 BEUC testing of user interface on YouTube taken on Pixel 9a Android device on 25 June 2025 and cross-checked on 28 July 2026.
17 BEUC testing of user interface on YouTube taken on Pixel 9a Android device on 25 June 2025 and cross-checked on 28 July 2026.

1.2. Steering

The Commission already imposed a non-compliance decision on Alphabet in July 2026 for failing to respect Article 5(4) DMA, which requires Alphabet **free of charge to allow app developers to communicate and promote offers** to, and **conclude contracts** with, consumers on channels beyond Apple's App Store.[18]

Alphabet had 60 days from that date to propose compliant changes, failing which it could be subject to periodic penalty payments. It is too early to tell if Alphabet is now compliant or not. BEUC has not seen any new proposals from Alphabet.

BEUC's main concerns prior to the non-compliance decision related to:

1. the **overlapping and extensive fees** Alphabet was charging app developers for steering;
2. the potential **non-neutrality of the information screen** that Alphabet required app developers to display every time they were steering a consumer outside the app environment;
3. the **level of discretion** Alphabet has in denying or revoking access to the External Offers Program[19], in which participation is essential to be able to engage in steering.

1.3. Tying

The DMA's Article 5(8) prevents gatekeepers from **tying** a core platform service to another core platform service, or to any other service which meets the DMA thresholds but is not designated as a core platform service. Article 13 DMA prevents any circumvention of this prohibition.

BEUC is concerned that Alphabet continues to use **several interface design and behavioural techniques** to undermine its compliance with the DMA's Article 5(8). This is prohibited under Article 13(4), while offering choices to consumers in a non-neutral manner is prohibited under Article 13(6). Some of the more prominent examples of non-compliance are below.

The first element relates to how Alphabet continues to disproportionately put forward Gmail options when the user is seeking to create a **Google Account for adults**. Although Gmail is not designated as a core platform service, it meets the thresholds for doing so. It must therefore comply with the ban on tying in the DMA.

However, during the user flow to create a Google Account which requires the use of an email address or a phone number, Alphabet provides **ready-made, available choices** of Gmail addresses as shown in Figure 4 (see below), or has Gmail **pre-selected** as the domain name in the box in the way that is shown in Figure 5 (see below). In so doing, Alphabet makes the Gmail option far more salient than the use of a third-party email address and leans on 'status quo bias' and users' preference for default options, knowing that many end users will use the easy option that is presented to them. This interface design undermines Alphabet's effective compliance with Article 5(8) DMA and thus likely breaches Article 13(4) DMA.

18 European Commission, *Commission fines Google €890 million for breaches of the Digital Markets Act* (23 July 2026, accessed 25 Sept 2026).

19 Google Console Play Help, *Developer Terms Of Service For External Offers Program* (published date unknown, accessed on 17 October 2025).

Figure 4: New Gmail address/third-party email address - With system suggestions[20]

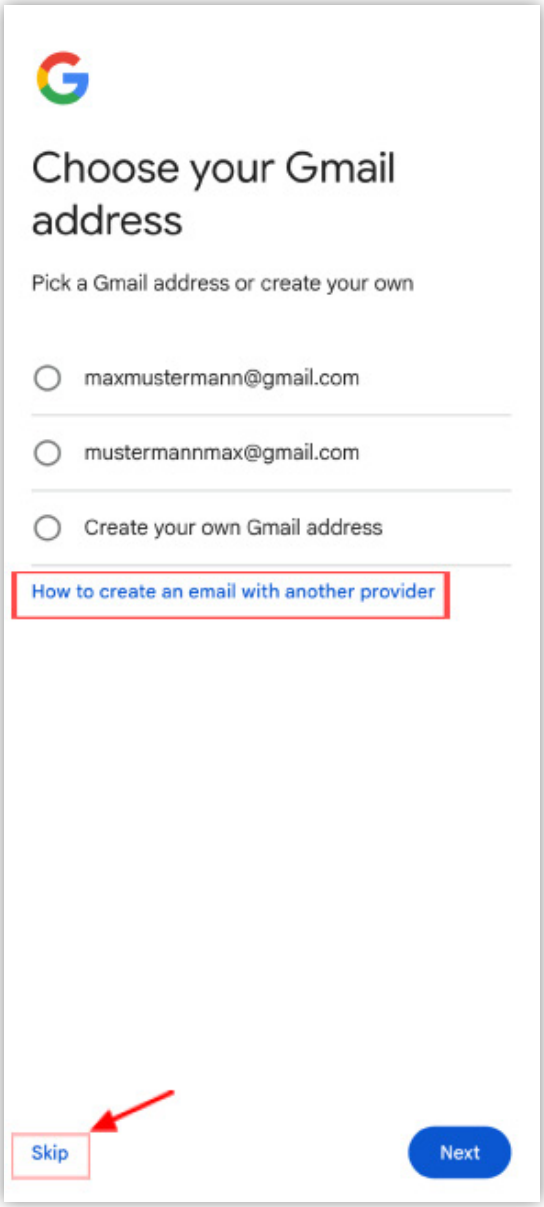
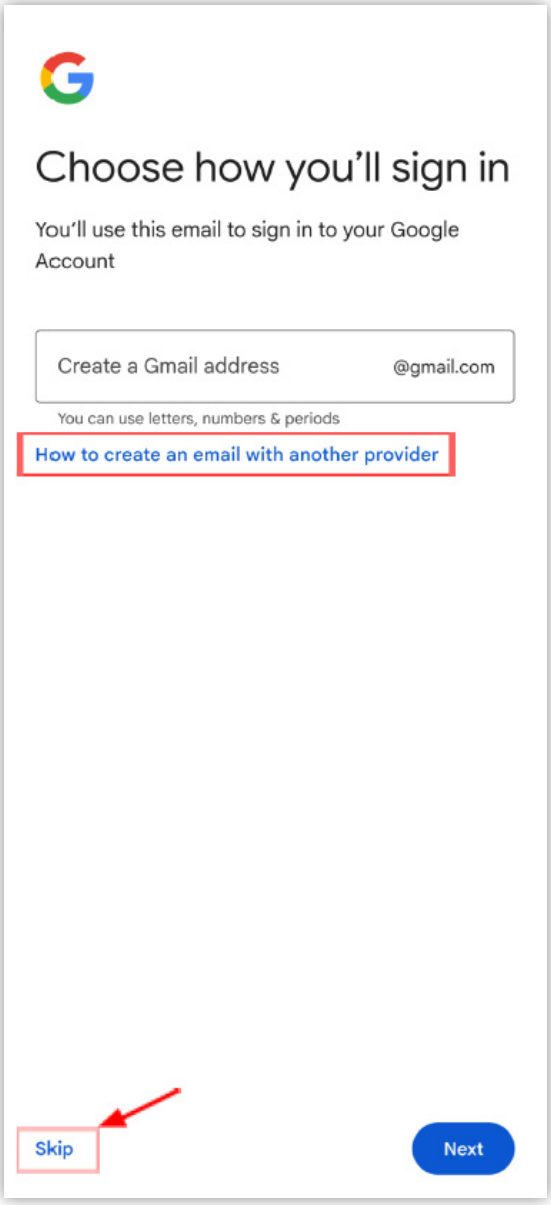


Figure 5: New Gmail/third-party email address - No system suggestions[21]



A second element relates to the **interface design for creating a child Google Account.** The flow is heavily skewed in favour of Gmail over the use of a third-party email address. This undermines the contestability of the market for email services and gives Alphabet/Gmail a heavy advantage in capturing a new generation of email users.

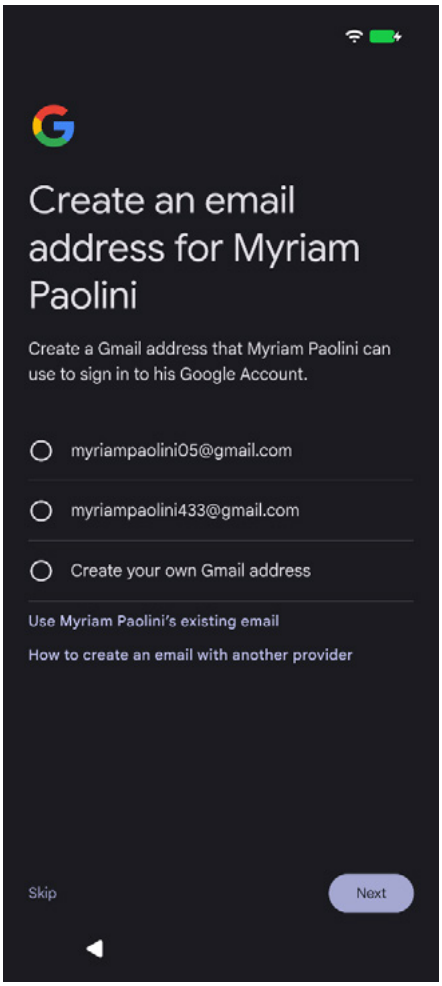
20 Alphabet, *Google's response to the European Commission's Request for Information dated 23 October 2025 (RFI 8) - Annex 1 - Google's revised solution for creating a regular Google Account - Initial setup of Android* (6 November 2025), pp. 13-14.

21 Alphabet, *Google's response to the European Commission's Request for Information dated 23 October 2025 (RFI 8) - Annex 1 - Google's revised solution for creating a regular Google Account - Initial setup of Android* (6 November 2025), pp. 13-14.

BEUC notes that the choices displayed to end users between using a Gmail address and a non-Gmail address are **not presented equally**. The options for creating or using a Gmail address are more prominent on the screen (larger font and more numerous) than the options to create or use a third-party email address (see figure 6). Alphabet also displays the option to use a third-party email address but it requires tapping on a link, which implies the process is both more complicated and time-consuming than if the user chooses to create a Gmail account.

Each of these interface design techniques is likely to influence the end user's decision-making by **increasing the likelihood that the end user will focus on the options which use Gmail,** rather than those of a third-party email provider, and likely breaches Article 13 DMA.

Figure 6: options for use of email address for child account on Google[22]



22 BEUC testing on Pixel 9a device on 20 November 2025 and cross-checked on 9 October 2026.

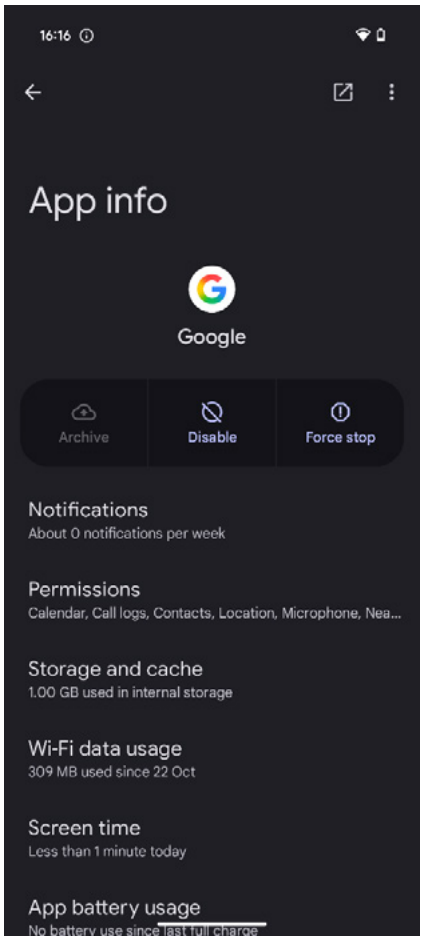
1.4. Uninstalling and setting alternative apps as defaults

Under Article 6(3) DMA, gatekeepers must allow consumers to **easily uninstall** any apps on their device and to **easily change default settings** on the operating system, virtual assistant or browser that steer them to other services provided by the gatekeeper. Related to the change of default settings, gatekeepers must prompt consumers to select their default search engine, browser or virtual assistant if any of these services have been designated under the DMA. Article 13 DMA prevents any circumvention of these obligations.

BEUC has multiple **concerns** with Alphabet's compliance with Article 6(3) DMA.

First, Alphabet prevents users from **uninstalling Google Search, Chrome, the Play Store, Google Maps or YouTube** on Pixel devices (see figure 7), on the basis that each of these core platform services came pre-installed on the device. It is unclear why an app that came pre-installed on a device cannot be uninstalled. On Pixel devices, the user is only capable of disabling these apps, but not uninstalling them altogether.

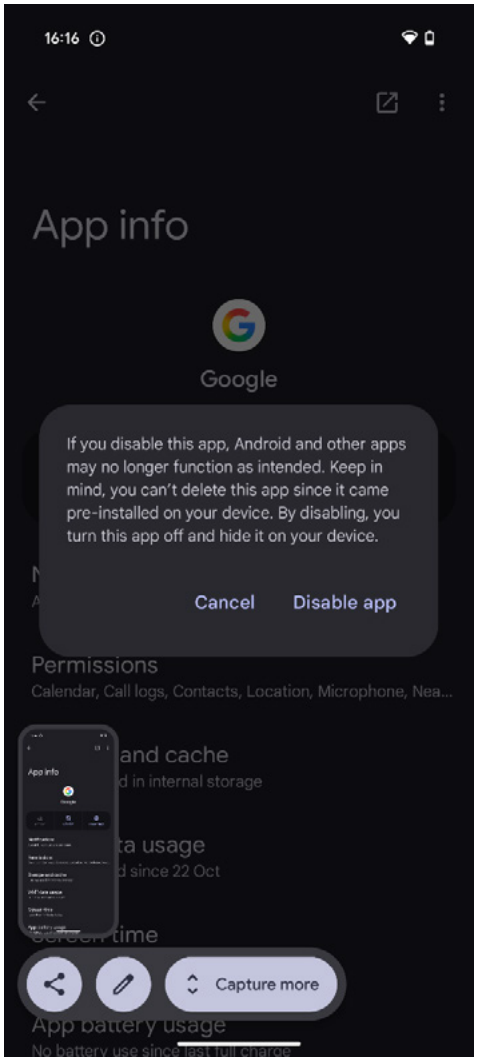
Figure 7: inability to uninstall Google Search on Pixel devices[23]



When the user attempts to disable Google Search, Chrome, YouTube, the Play Store or Google Maps, a scare screen appears (see figure 8) that says *"Android and other apps may no longer function as intended."* This scare screen has the **likely effect of chilling end users from disabling the apps** by raising fears that the device will no longer function correctly. Unless Alphabet can substantiate why Android may no longer function as intended and why its effective compliance with Article 6(3) DMA constitutes too large a risk, BEUC considers such behaviour to likely constitute non-compliance with Article 6(3) DMA.

23 BEUC testing of uninstallation of Google Search on Pixel 9a device on 30 October 2025.

Figure 8: scare screen displayed when trying to disable Google Search on Pixel devices[24]



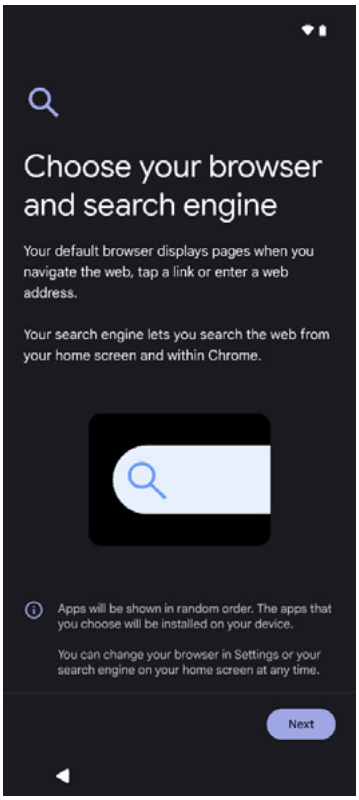
Even after the user has selected an alternative search engine from the DMA-required choice screen, it is **only by disabling Google Search that certain access features on the device no longer lead to Google Search**. For example, the Circle-to-Search feature, which activates by holding down the bottom of the screen on a Pixel device, still leads to Google Search even after selecting a third-party search engine as default. This feature should be equally accessible to third-party search engines, just as it is to Google Search. That such a feature still leads end users to Google Search, rather than the default search engine, undermines Alphabet's compliance with this provision and may also be a breach of the Article 6(7) DMAon interoperability.

Second, Alphabet uses **behavioural techniques and non-neutral interface design,** as well as **technical barriers**, to undermine its compliance with the DMA relating to browser choice, at least on Pixel devices.

In the user flow to select the default browser on Pixel devices, Alphabet mentions Chrome in the first information screen before proceeding to the choice screen (see figure 9 below). This mention likely **primes end users to select Chrome in the upcoming browser choice screen** to the detriment of third-party browsers. This is a well-known behavioural technique that likely falls foul of Article 13.

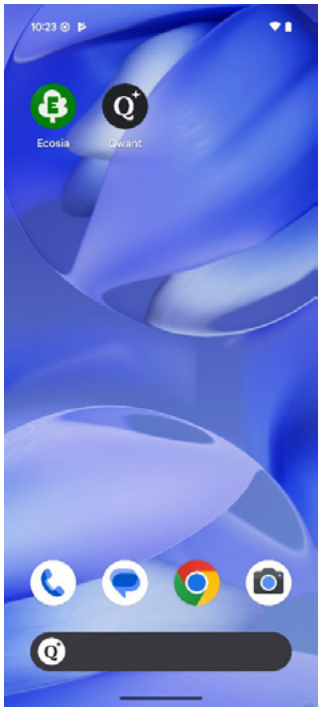
24 BEUC testing of uninstallation of Google Search on Pixel 9a device on 30 October 2025 and cross-checked on 7 October 2026.

Figure 9: screenshot of information screen announcing the upcoming choice of browser and search engine[25]



On Pixel devices at least, **Chrome remains in the dock** even after the user has selected an alternative default browser (see figure 10). This ensures that Alphabet continues to provide high visibility to Chrome even though the user has selected an alternative browser. Although the browser in the dock can be manually changed, people are subject to status quo bias **as recognised by the EU General Court in the Google Android case**[26] and tend not to do this. Alphabet can rely on status quo bias to undermine the effectiveness of the choice screen and this behavioural technique should therefore not be allowed.

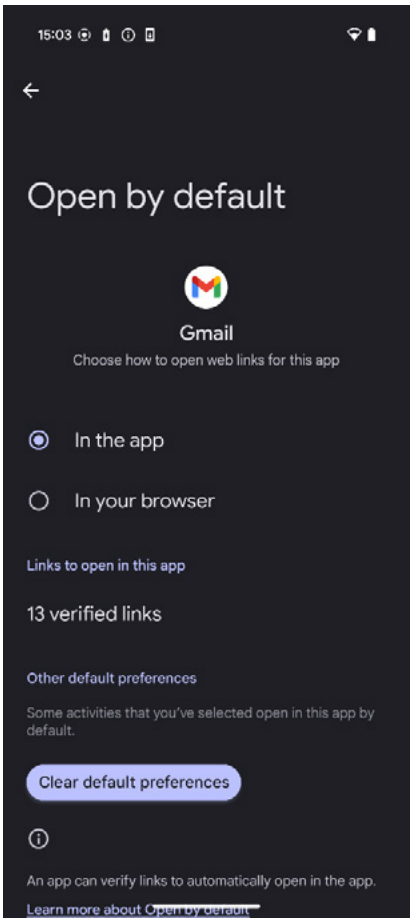
Figure 10: screenshot of Chrome in dock despite having selected alternative browser as default[27]



25 BEUC testing of browser and search engine choice screen on Pixel 9a device on 25 June 2025 and cross-checked on 7 October 2026.
26 *Google LLC and Alphabet, Inc. v European Commission* (Judgment) [22 September 2022] Case T-604/18, ECLI:EU:T:2022:541.
27 BEUC testing of browser choice screen on Pixel 9a device on 25 June 2025 and cross-checked on 7 October 2026.

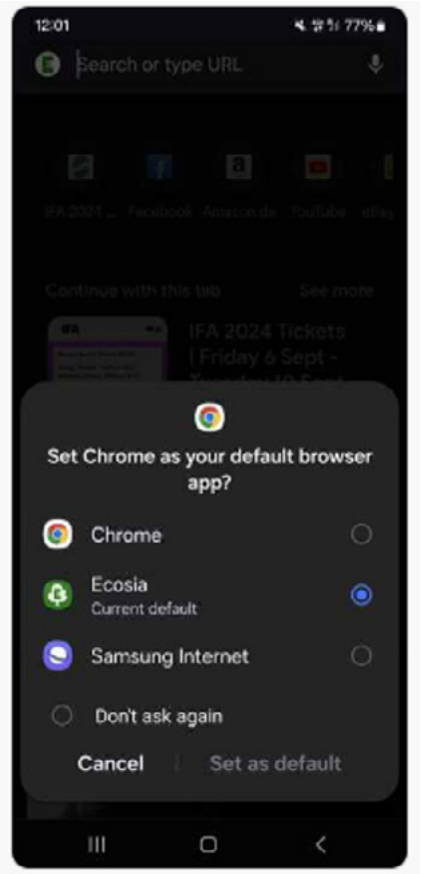
Third, on Pixel devices, Alphabet has a setting which **by default opens links from Gmail in the app rather than in the default browser.** It is only by tapping on the individual settings for Gmail and clicking on the "*Open by default*" menu item that the user is able to clear the default setting that certain activities open in Gmail by default (see figure 11). The fact that this option is activated by default and hidden away in a menu for that specific app implies that **it is not easy for end users to change their default settings** as required under Article 6(3).

Figure 11: changing default of opening links in Gmail[28]



Fourth, Alphabet regularly displays **prompts** to users to switch their default browser or search engine to Chrome and Google Search after they have chosen an alternative (see figure 12). Although it is difficult to know how frequently Alphabet displays these prompts, it is obvious that their **repeated use can undermine the ability of the user to easily change their default settings** on their device and thus breach the DMA. This is an area where the Commission should issue guidelines to clarify which kinds of behaviour from a gatekeeper would be considered acceptable and which would not. Alphabet should also provide greater transparency about how often it has displayed prompts to a user on a particular device.

Figure 12: prompt to switch to Chrome even though Ecosia has previously been set as the default browser[29]

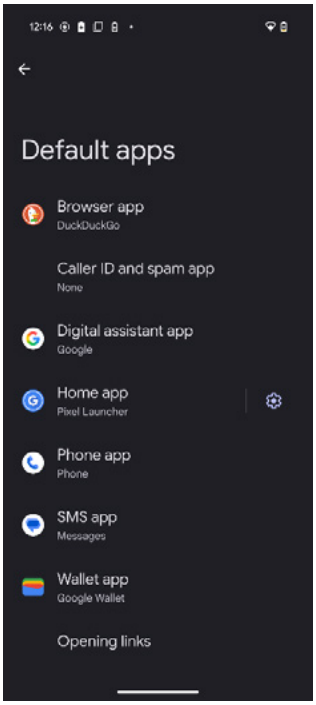


28 BEUC testing on Pixel 9a device on 31 October 2025 and cross-checked on 7 October 2026.
29 Screenshot taken of prompt to switch from Ecosia to Chrome on Samsung device on 23 May 2025.

Fifth, it is unclear if Alphabet has now rolled out a compliant browser/search engine choice screen to **all legacy and new devices, Android or other, at least once**. Alphabet's messy rollout, which involved initially displaying a stratified randomisation list of providers in its choice screens instead of a fully randomised list[30], and the absence of choice screens altogether on devices running on Android 12 or earlier versions from March 2024 at least until June 2025,[31] has undermined Alphabet's compliance with Article 6(3) DMA. For the sake of clarity in compliance, BEUC would recommend that all Android and non-Android devices should have to display a compliant choice screen again.

Finally, BEUC does not believe it is easy to change the default settings on certain Android devices. BEUC carried out testing on a Pixel 9a device to see how easy it was to install and set several apps across different app categories as defaults. In the "*Default apps*" settings, it isn't possible to set an **alternative maps app** as the default on the device, nor is it possible to do so for an **alternative email app** (see figure 13 for the list of apps which can have alternative default options).

Figure 13: default apps options in "Settings"[32]



1.5. Alternative app stores and sideloading

The DMA (Article 6.4) requires gatekeepers to **allow and technically enable the installation of third-party apps and app stores through any distribution channel.** Gatekeepers should also allow users to easily set these apps and app stores as the **default** option across the user's device. Gatekeepers can put in place security restrictions, provided they are proportionate and justified. Article 13 DMA prevents any circumvention of this prohibition.

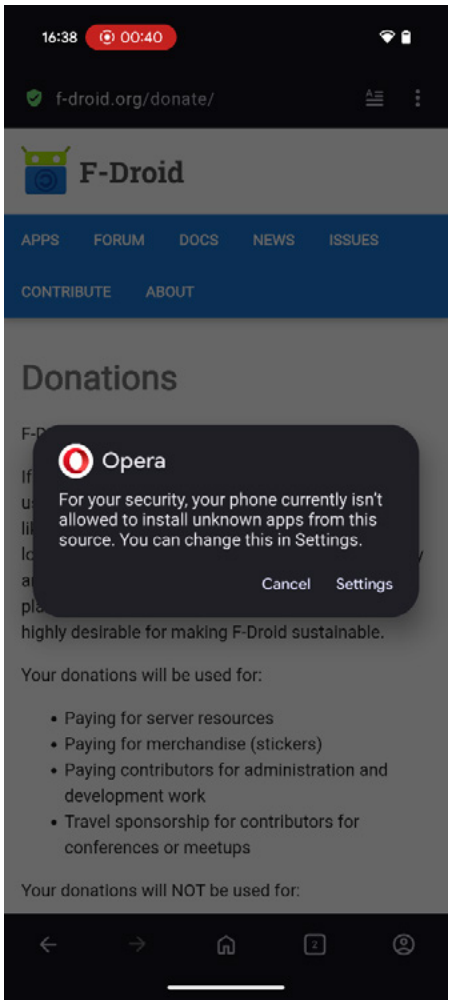
BEUC has concerns that Alphabet introduces **unnecessary hurdles and non-neutral elements** in the process to download an alternative app store. These practices create **negative friction** for users which may dissuade them from continuing the process and thus may breach the DMA.

30 Alphabet, *EU Digital Markets Act (EU DMA) Compliance Report Non-Confidential Summary* (6 March 2026, accessed on 6 October 2026), pp. 137-8.
31 Alphabet, *EU Digital Markets Act (EU DMA) Compliance Report Non-Condential Summary* (7 March 2025, accessed 25 June 2025), page 115.
32 BEUC testing on Pixel 9a device on 31 October 2025 and cross-checked on 7 October 2026.

First, the default setting, at least on a Pixel device, is that the user must first change their settings to allow the download of a third-party app store (see figure 14).

It is unclear why Alphabet **deactivates** this setting **by default** when end users are meant to be able to download third-party app stores under the DMA. Furthermore, Alphabet gives end users the impression that this is a browser setting, by displaying the chosen browser's logo (see figure 14), when it is in fact an **Android setting by default** because this message appears regardless of the default browser the end user has selected.

Figure 14: downloading a third-party app store first requires a change in default settings[33]

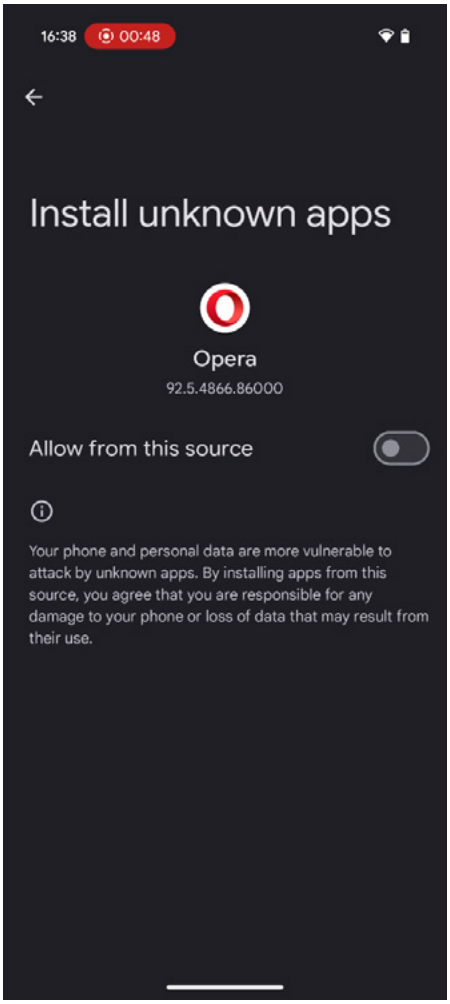


Second, Android displays **non-neutral interfaces** and uses **behavioural techniques** when the user attempts to install a third-party app store. The use of such interfaces and techniques may breach Article 13 DMA. The first example is displayed in figure 14 above. By referring to security risks and *"unknown apps"*, Alphabet creates a sense of insecurity among users who may begin to doubt how safe the installation of a third-party app store may be. Alphabet should use more neutral wording.

Alphabet uses alarmist language when, at the next step, users tap on the settings option to activate the possibility to download a third-party app store. Alphabet displays a scare screen (see figure 15). The heading *"Install unknown apps"* as well as the accompanying information which reads *"Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use"* will likely have a **serious chilling effect** on end users who may be interested in downloading a third-party app store. This information is neither objective nor balanced. Again, this is a message Alphabet requires, not the third-party browser, because it displays regardless of the browser selected.

33 BEUC testing on Pixel 9a device on 14 November 2025 and rechecked on 9 October 2026.

Figure 15: changing default settings to be able to download third-party app store[34]



Users appear to have to go through the same process when downloading a third-party app from the just downloaded alternative app store. The end user has the same scare screen and worrying language displayed when they try to toggle the setting to activate downloads from an already authorised third-party app store to be able to download an app from it.

Finally, it does not appear, at least on Pixel devices, that it is possible to set a third-party app store **as the default app store across the device**. This directly contradicts Article 6(4) DMA and should be remedied immediately by the European Commission or gatekeepers.

1.6. Self-preferencing

Under Article 6(5) DMA, **gatekeepers cannot treat their own services or products more favourably in ranking, indexing or crawling** than similar services or products offered by a third party. The gatekeeper must also apply transparent, fair and non-discriminatory conditions to the ranking. The DMA's Recital 52 clarifies that the provision applies to any measure that has an equivalent effect to differentiated or preferential treatment in ranking, while Article 13 DMA prevents any circumvention of this obligation.

The European Commission found that Alphabet breached Article 6(5) DMA in its Non-Compliance Decision[35] of 23 July 2026. Alphabet had 60 days from that date to enter into compliance.

34 BEUC testing on Pixel 9a device on 14 November 2025 and cross-checked on 29 October 2026.

35 European Commission, *Commission fines Google €890 million for breaches of the Digital Markets Act* (23 July 2026, accessed on 12 June 2026).

While Alphabet has in the meantime made some positive steps towards compliance and released a new layout to Google Search results pages, it remains clear that Alphabet **still fails to comply** with the Commission's decision overall.

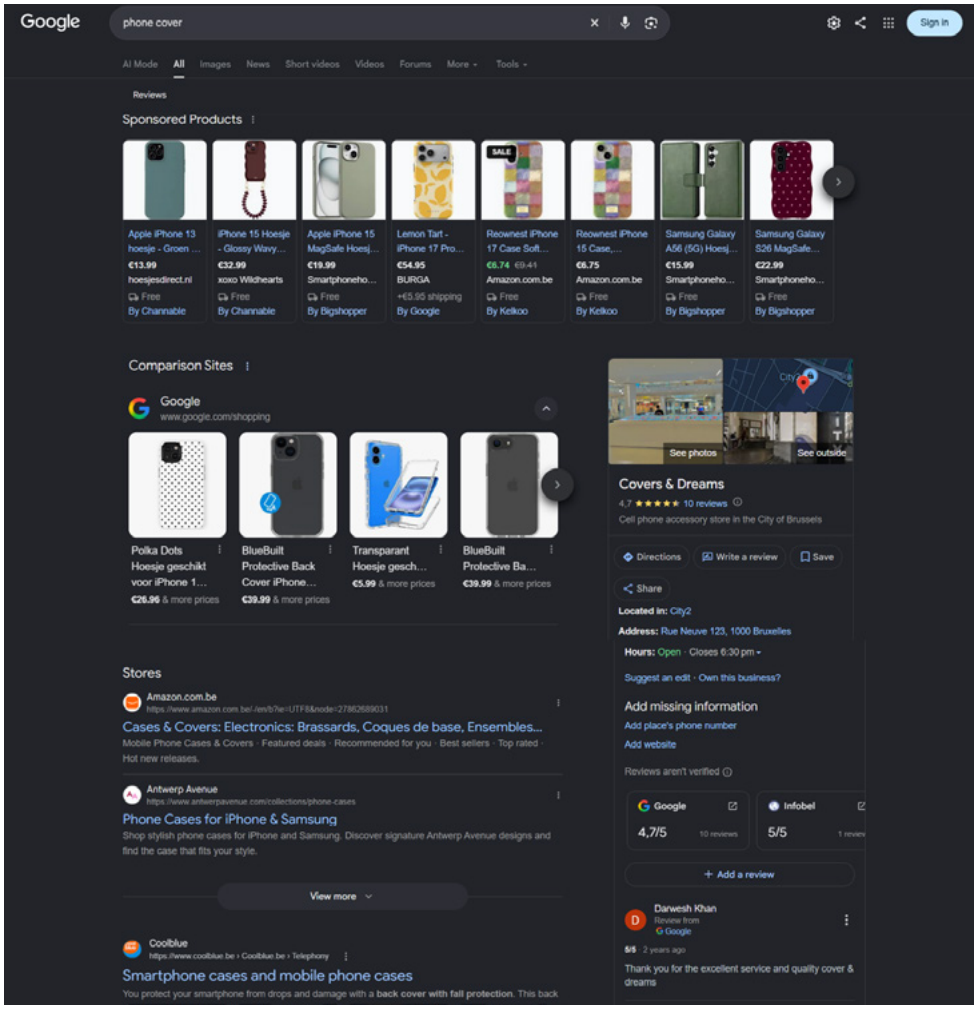
First, at least relating to **shopping services, Alphabet continues to give greater prominence to its product ads unit (**"Sponsored products") compared to any similar comparison-shopping service belonging to third parties (see figure 16 below). As the Commission's decision makes clear, the product ads unit in its current configuration constitutes a comparison-search service that goes beyond the role of a search engine. Its display at the top of the Google Search results page gives it prominence that no rival third-party service can compete with.

Second, Alphabet appears to **systematically display its own comparison service in the products unit** of Google Search, whether for hotels, shopping, flights or any other service addressed in the decision. However it does not grant the same degree of visibility to individual third parties given that only a handful are displayed at a time in an accordion. Worse, it appears, at least for shopping services, that Alphabet regularly only displays its own service in the 'Comparison Sites' unit (see figure 16 below).

Third, Alphabet continues to display results for product units using **Google Maps** on Google Search rather than also allowing the display of alternative maps services.

Fourth, Alphabet continues to display its own **translation or sports services** prominently at the top of the Google Search results pages, depriving rival third-party services from achieving the same level of prominence.

Figure 16: Google Search results page following query for 'phone cover'[36]



Given the extent and duration of the non-compliance, BEUC recommends that the Commission impose periodic penalty payments.

36 BEUC testing on HP desktop running on Windows on 12 October 2026.

2. Amazon

2.1. Consent for use of personal data

The DMA's Article 5(2) requires gatekeepers to seek consent from consumers before:

1. Combining their personal data from first and third-party sources for ads purposes;
2. Combining their personal data from the gatekeeper's core platform service with any other service;
3. Using their personal data from the gatekeeper's core platform service in another service provided by the gatekeeper;
4. Signing them in to other gatekeeper services to combine their personal data.

The DMA's recitals lay out further conditions, while Article 13 DMA prevents circumvention and consent must meet the criteria laid out in the GDPR.

Amazon uses two prompts to attempt to comply with these various provisions: an Amazon Store prompt (see figure 17) and an Amazon Ads prompt (see figure 18). **Neither is likely to satisfy the requirements** set out in the DMA.

BEUC takes the view that both Amazon's consent screens, which have changed only minimally since 2024, continue to use **behavioural techniques** and **interface designs** to steer users towards the options that Amazon favours. Their use likely falls foul of the DMA because they may undermine effective compliance with Article 5(2) DMA.

The texts Amazon uses in the interfaces consistently place the option to consent in a positive light, which is neither balanced nor objective. The texts also use vague terms instead of clearer ones such as 'personal data', while the use of brightly coloured buttons for the option to consent is a clear behavioural technique to make the 'consent' option more salient.

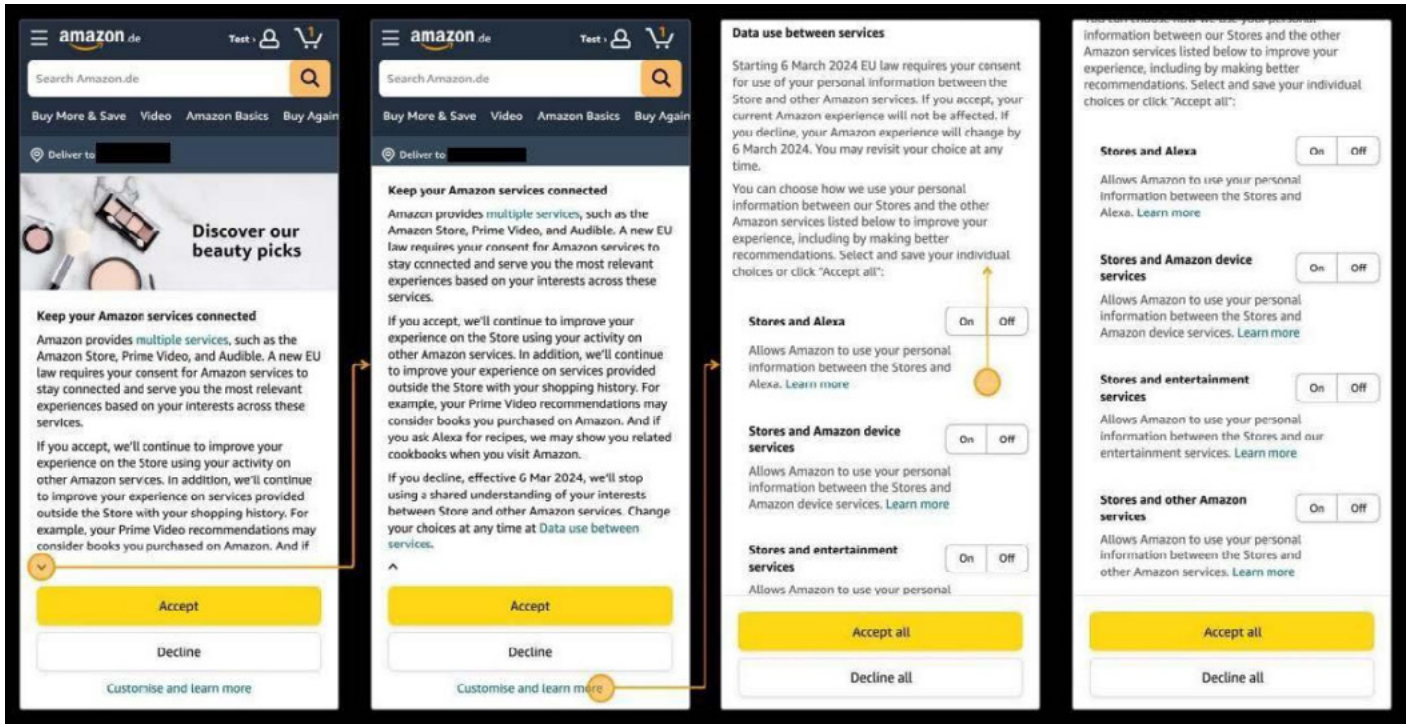
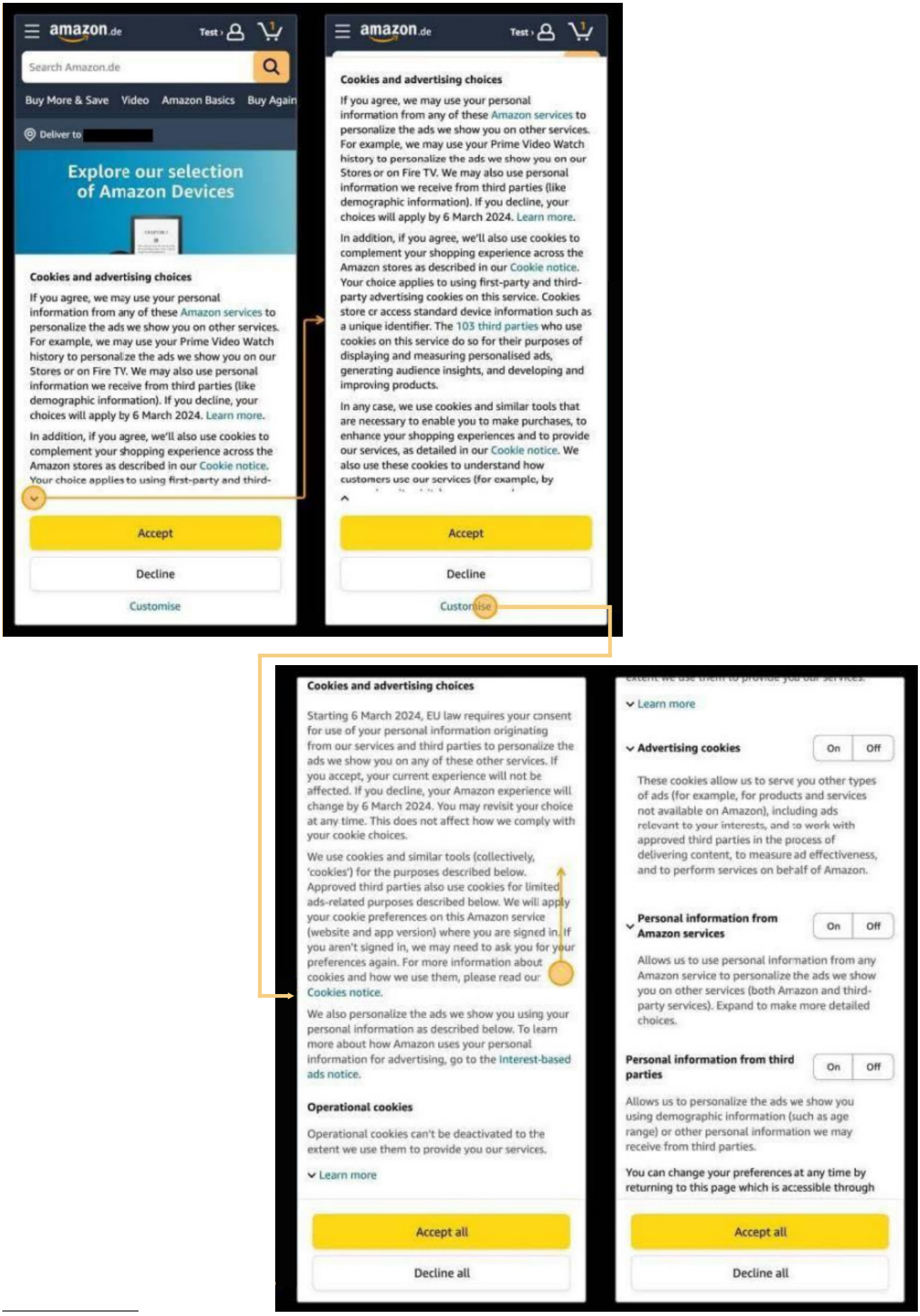


Figure 17: Amazon Store Prompt[37]

37 Amazon, *DMA Compliance Report* (5 March 2026, accessed 24 August 2026), page 8.

Figure 18: Amazon Ads Prompt[38]



38 Amazon, *DMA Compliance Report* (5 March 2026, accessed 24 August 2026), page 9.

2.2. Price controls

Article 5(3) DMA prohibits gatekeepers from limiting the ability of business users to offer the same goods they offer on the gatekeeper's platform at different conditions, including price, on other channels.

Recital 39 DMA specifies that this restriction *applies "...to any measure with equivalent effect, such as increased commission rates or de-listing of the offers of business users."*

Although Amazon no longer appears to use so-called 'parity clauses' in its terms with third-party sellers, BEUC is concerned that **Amazon's price controls**, as detailed in its compliance report,[39] may constitute a breach of Article 5(3) DMA because of their possible equivalent effect.

Amazon explains that **it uses monitoring tools which check the prices at which a third party is selling its products off-Amazon**. When Amazon finds a product that is on offer elsewhere for less, Amazon applies three potential types of penalties for that product on its own marketplace:

1. If the product is available at a lower price on a competing online intermediation service, the product can no longer be displayed as a Featured Offer or Second Displayed Offer on Amazon, both of which are privileged positions in terms of visibility and for concluding a contract with the end user.
2. If the product is available on Amazon but Amazon considers it *"priced significantly higher than the typical price for that item"*, the product will no longer be displayed as a Featured Offer or Second Displayed Offer on Amazon.
3. If the product is available on Amazon at *"egregiously high prices"*, the offer will be removed from listings to consumers.

These 'price controls' appear to be **unilateral mechanisms to downgrade the visibility of products where there are price differences**, or significant price differences, between the prices offered on Amazon and those offered on third-party channels. Amazon does not provide explanations as to how it determines what is a significant or egregious price difference. In addition, this conduct has already fallen foul of Germany's Section of the German Competition Act.[40]

Each of these may be problematic for several reasons, which are assessed in turn:

a) Lower prices off-Amazon exclude product from Featured Offer or Second Displayed Offer on Amazon

While Amazon claims in its compliance report that this measure is targeted at third-party online intermediation services and does not limit the freedom of sellers on its platform, it is difficult to see how such a policy does not have a substantial effect on sellers who sell on both Amazon and at least one other third-party online intermediation service.

The Featured Offer and Second Displayed Offer boxes are prime real estate in terms of visibility on Amazon. When an offer features in either of these two boxes, it receives enhanced visibility and is the offer most likely to lead to the conclusion of a contract.

Removing the possibility of featuring in these boxes is likely to have a detrimental effect on the seller of that product who will find themselves with lower sales on Amazon. The seller will therefore face the choice of either accepting that their products should be on sale on Amazon and on other third-party online intermediation services for similar prices, or forsake a substantial number of Amazon sales and rely on the third-party intermediation service to make up for the difference. Because of Amazon's gatekeeper position on the European market for intermediation services, it is more likely to be the former.

This conduct therefore has the **equivalent effect of limiting sellers' freedom from offering their goods at different prices on other channels** and is therefore likely to breach Article 5(3) DMA.

It is important to protect competition on retail prices in order to ensure consumers have access to products that reflect market prices and not those of gatekeepers. If Amazon is able to force rival intermediation services to align their prices on Amazon's, it means that the commissions Amazon charges sellers cannot be challenged by competitive means. This would have **adverse consequences for the fairness and contestability of online intermediation services.**

---

39 Amazon, *DMA Compliance Report Non-Confidential Version, Annex 1* (5 March 2026, accessed 24 August 2026), pp. 5-7.

40 Bundeskartellamt, *Bundeskartellamt prohibits Amazon from applying so-called price control mechanisms and orders the disgorgement of 59 million euros in economic benefits* (5 February 2026, accessed 14 October 2026).

b) Significant price differences from 'typical price' exclude product from Featured Offer or Second Displayed Offer on Amazon

The same reasoning applies here as for sub-section 1 regarding why Amazon's restrictions on the Featured Offer or Second Displayed Offer may be detrimental to the fairness and contestability of the online intermediation services market.

However, a further complication is that Amazon fails to explain what a "*significantly higher than the typical price for that item*"[41] is deemed to be, or what the parameters are for establishing that threshold. For instance, does Amazon use the price advertised on the seller's own channel as a metric? What other parameters does Amazon use? Even if the seller's own channel is not included, it would appear to constitute a limitation on the ability of sellers to offer their products through third-party online intermediation services at prices that are different from those offered by the gatekeeper.

Without substantially more detailed and clearer explanations about Amazon's pricing policy, it may be the case that Amazon is breaching Article 5(3) DMA.

c) Delisting following display of "egregiously high prices"

While there may be some merit to delisting offers which engage in price gouging, the risk exists of Amazon applying this policy too widely to restrict competition of rival third-party online intermediation services which allow a seller to offer their goods at lower prices than on Amazon.

Once again, Amazon fails to disclose the threshold at which it deems an offer to be at an "*egregiously high price*" or what parameters it uses to determine that threshold.

41 Amazon, *DMA Compliance Report Non-Confidential Version, Annex 1* (5 March 2026, accessed 24 August 2026), p. 5.

3. Apple

3.1. Steering

The Commission has already imposed a Non-Compliance Decision on Apple in April 2025 for failing to respect Article 5(4) DMA, which requires Apple free of charge to allow app developers to communicate and promote offers to, and conclude contracts with, consumers on channels beyond Apple's App Store.

Apple has appealed this decision before the EU's General Court (T-438/25) and BEUC is a third-party intervenor in the case in support of the Commission decision.

In the meantime, Apple and the Commission had been locked for many months in regulatory dialogue to resolve the issue. After several rounds of changes proposed by Apple, Apple announced new terms on 18 August 2026[42] which the Commission welcomed and which will be operational from 1 October 2026.

Its main terms are:

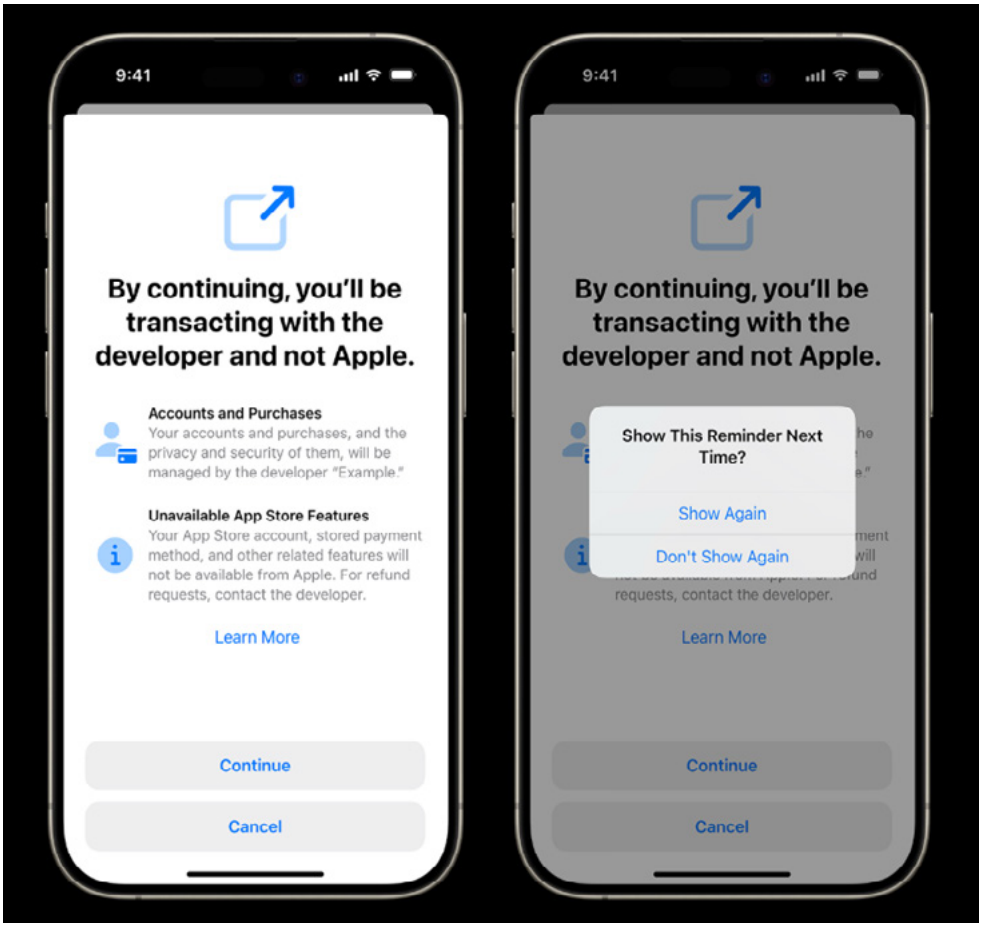
- One set of terms for all app developers providing digital content/services which replaces all previous terms.
- Commissions of:
    - 15% (or 10% for small businesses and Apple program parters) on steering to offers outside the App Store, which include to apps, websites or third-party app stores, excluding auto-renewing transactions after the first year;
    - 20% (or 10% for small businesses and Apple program parters) on sales through the App Store but using an alternative payment mechanism;
    - 26% (or 15% for small businesses and Apple program parters) on sales through the App Store and using Apple's In-App Purchase;
- Apps in the children category are subject to restrictions on payments which do not use Apple's in-app purchase system.
- Third-party app stores and app developers distributing directly from their website must meet one of a number of criteria to be distributable on iOS;

Apple also requires the display of an "*In-App Disclosure sheet*" when an app developer seeks to steer a consumer outside the app environment. Although the disclosure sheet (see figure 19), which dates from 2025[43], marks a substantial improvement on previous scare screens that Apple forced app developers to display, it still plays on the **recognised human behavioural biases** of 'loss aversion' and 'status quo' in the text in the second block under the heading in bold "*Unavailable App Store Features*."

This wording suggests that end users will lose something, which may make some consumers reluctant to continue and choose instead to stick to Apple's App Store environment. It contrasts markedly with the overall bolded heading and the wording of the first text block which are a more neutral, objective description of the situation – that the user will be transacting with a developer rather than Apple. This objective information does not imply a loss of availability of features, unlike the wording in the second block.

42 Apple, *Apple announces changes for apps in the European Union* (18 August 2026, accessed 26 August 2026).
43 Apple, *Communication and promotion of offers on the App Store in the EU* (unknown date, accessed on 26 August 2026).

Figure 19: Apple's In-App Disclosure Sheet[44]



It is also unclear if Apple is maintaining or changing the text that appears if a consumer clicks on the "*Learn More*" link compared to the version BEUC saw in 2025.

Apple's lengthy description on that page in 2025 focused on features that consumers would lose access to if they made an external purchase with the app developer, heavily drawing on the recognised human behavioural bias of 'loss aversion'. In that text, Apple also played on consumers' fears by choosing to highlight several times how acute the risk of fraud was outside the App Store. The "*Learn More*" text amounted to a scare screen which would likely have the effect of cooling the end user's willingness to proceed with making an external purchase.

By using behavioural techniques which could undermine effective compliance with Article 5(4) DMA, Apple may be breaching Article 13(4) while the use of potentially non-neutral interfaces breaches Article 13(6) DMA.

Beyond the disclosure sheet, the new terms Apple announced in August 2026 have been met with incredulity from major app and games developers. For instance, the Coalition for App Fairness and the European Games Developer Federation said in a joint letter about Apple's fees that: *"most app developers cannot afford to absorb them, meaning rival stores and lower-cost offers risk being taxed out of existence before they can take root."*[45]

While BEUC is not best placed to argue what fee amount payable to Apple would be considered acceptable for facilitating the initial transaction between the app developer and end user, two things are obvious. First, **Apple cannot charge for the act of steering itself** which must remain free of charge as Article 5(4) DMA states. It is unclear how Apple's fees comply with this precise point. Second, if Apple sets too high an initial acquisition fee, and which is not commensurate with the cost of facilitating that initial transaction, **consumers will not be able to benefit from the full possibilities that steering allows in the EU.**

BEUC is concerned that the terms announced in August 2026 do not sufficiently improve the situation compared to the pre-DMA situation and leave questions unanswered regarding Apple's compliance with the DMA.

---

44 Apple, Webpage: 'Communication and promotion of offers on the App Store in the EU' (unknown date, accessed on 26 August 2026).
45 Various, *Joint letter: Apple's New EU App Store Terms Still Fail the DMA* (8 Sept. 2026, accessed on 22 Oct. 2026).

3.2. Alternative app stores and sideloading

Apple has been under investigation by the Commission since June 2024 for potential breach of Article 6(4) DMA.[46] This provision requires Apple to enable the installation of third-party apps and app stores through means other than Apple's App Store. The gatekeeper can put security measures in place to protect the integrity of the device, provided these are proportionate and justified.

Under the same deal mentioned in sub-section 6.1, Apple has put forward new terms for the installation of apps and app stores through alternative channels in August 2026. There are two concerns: fees and user experience.

First, on fees, it is unclear whether Apple's 5% commission on the sale of any digital goods or services in an app that has been installed through an alternative app store is prohibitively high. However, what is clear is that if this fee is prohibitively high for app developers/third-party app stores and does not reflect the cost of Apple running the operating system for that app/app store, it could **deprive consumers of the possibility of turning to alternative app stores** on iOS or iPadOS altogether.

Second, only some of the new user flows for the installation of apps and app stores have been released by Apple in August 2026. [47] These user flows have not changed from the proposals Apple made to the Commission in 2025, in which BEUC had already detected problems. These issues should be addressed to **avoid unnecessary negative friction points** during the installation process of apps and app stores through alternative channels.

To initiate the downloading of app stores from the web (see screen 2 of figure 20 below), Apple continues to require the display of the legal entity's name seeking the download of the app store, rather than simply displaying the website's or app store's name, which consumers will be more familiar with. BEUC is concerned that this could **weaken the link the consumer makes with the app store that they are interested in downloading** if a name they do not recognise is displayed. For example, the greater the difference between the name of the legal entity and the website/app store, the higher the likelihood that the consumer is confused or worried and does not complete the download of the alternative app store. We know from US court documents in US Case Epic Games Inc. v. Apple Inc.[48] that Apple employees deliberately played on this fact when designing a user interface that would be employed as part of the steering process in the US: *"One employee further wrote, "to make your version even worse you could add the developer name rather than the app name." (CX-206.4.)""*

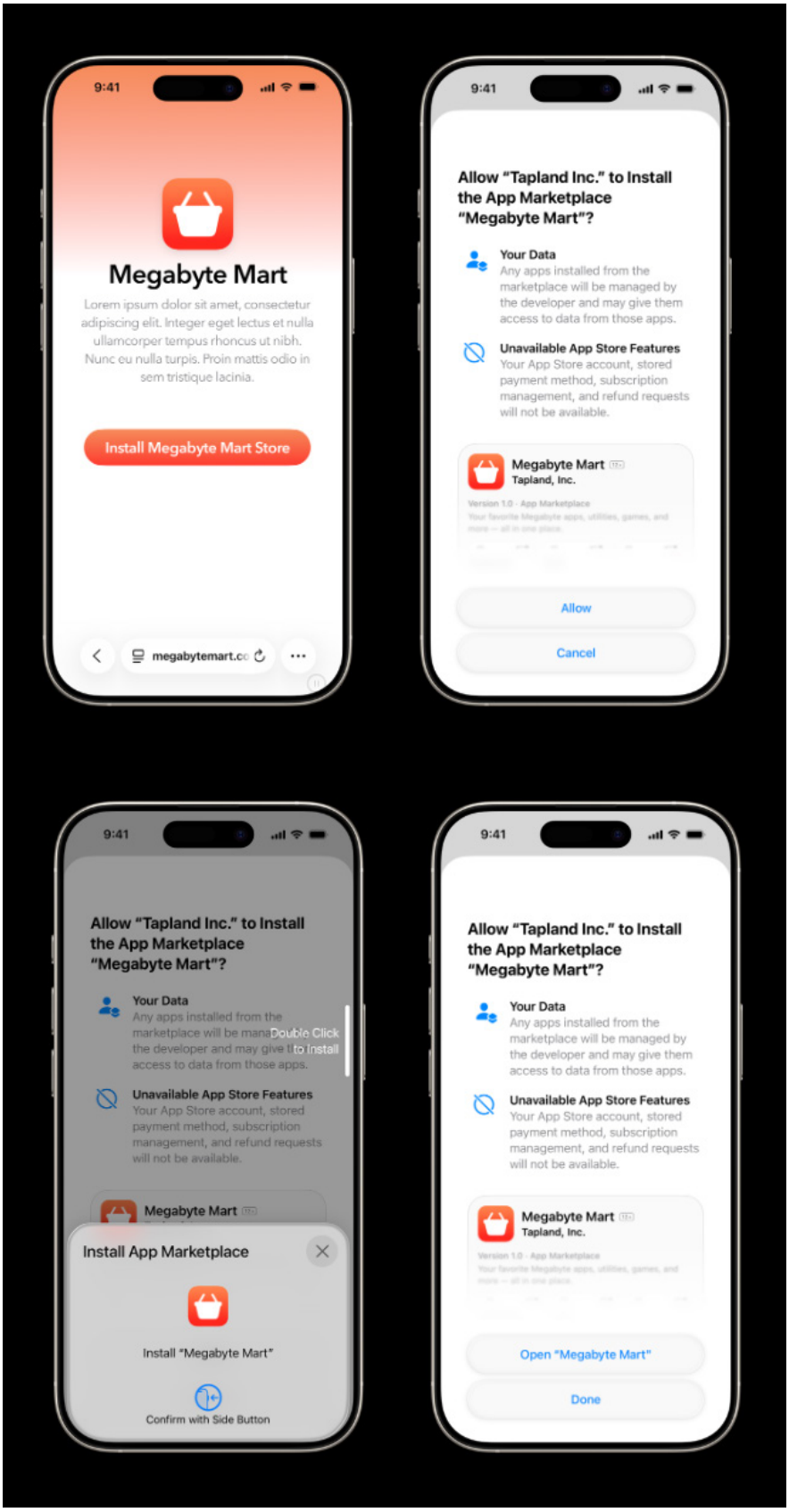
BEUC is also concerned that screen 2 (see figure 20) heavily draws on the **recognised human behavioural bias** of 'loss aversion' in the description for "*Your Data*" and "*Unavailable Features*". The interface may have the effect of cooling the end user's willingness to proceed with the download because Apple is describing features that the user could lose, or certain risks that could emerge ("*...may give them access to your data*"), which is non-neutral information, while failing to mention any possible benefits.

46 European Commission, *Commission sends preliminary findings to Apple and opens additional non-compliance investigation against Apple under the Digital Markets Act* (24 June 2026, accessed 26 August 2026).

47 Apple, *Alternative distribution installation experience updates* (date unknown, accessed on 26 August 2026).

48 United States District Court - Northern District Of California, *Epic Games Inc. v Apple Inc*. Case No. 4:20-cv-05640-YGR, 30 April 2025.

Figure 20: user flow for downloading an alternative app store from the web[49]



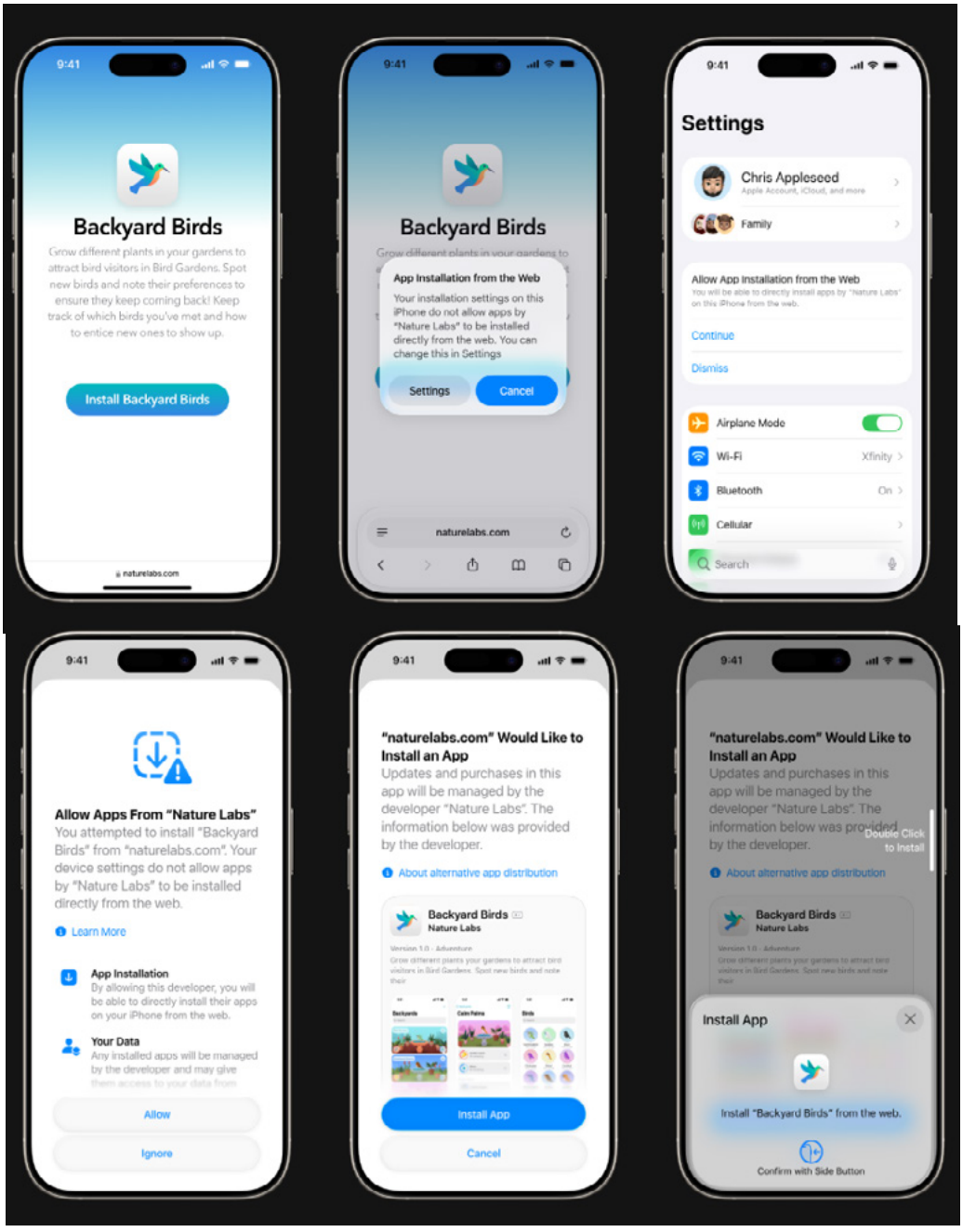
49 Apple, Alternative distribution installation experience updates (date unknown, accessed on 26 August 2026).

Regarding the downloading of apps from the web (see figure 21), the same potential point of friction appears in requiring the use of the name of the legal entity behind the website, though it is less marked than for the installation of alternative app stores because the interfaces confusingly also occasionally mention the website name.

The **number of screens** used in the user flow also appears **excessive** and should be simplified. For example, rather than requiring the user to manually change the settings on their device to allow apps to be downloaded from the web in screen 3, screen 2 could simply display buttons which allow the change to be made directly when tapping on a button, which would read *"Allow"* rather than *"Settings."* Screens 3 and 4 would then be redundant and could be removed. Changes such as these matter because **every step and screen inserted into the user experience creates friction** which reduces the likelihood that the consumer completes the initial task of downloading an app from the web.

As with the downloading of app stores from the web, it is important that the information displayed to the user on screens 4 and 5 should be **neutral**, which means the texts should be balanced and objective and be devoid of behavioural techniques. It is unclear from the fold of the screen precisely what text is displayed, but the texts should be changed if they are non-neutral or use behavioural techniques. The same goes for the text which would be displayed under the *"Learn More"* button.

Figure 21: user flow for downloading apps from the web[50]



50 Apple, *Alternative distribution installation experience updates* (date unknown, accessed on 27 August 2026).

3.3. Interoperability with the gatekeeper's operating system

Under Article 6(7) DMA, the gatekeeper must allow effective interoperability free of charge between third-party providers of services and/or hardware on the one hand and the gatekeeper's operating system or virtual assistant on the other, so that the former can access the same hardware and software features as are accessible to the gatekeeper's own services or hardware. The gatekeeper is allowed to take security measures to avoid compromising their operating system, virtual assistant, hardware or software, provided they are proportionate and justified to the Commission.

The Commission and various third-party business users found Apple's first attempts to comply insufficient. As a result, the Commission published two sets of specifications[51] which intended to clarify how Apple needed to comply with Article 6(7). Most of the measures outlined had deadlines over the course of 2026.

The list of interoperability requests made by third parties[52] shows that many of them are being rejected by Apple, in large part because Apple deems them to be outside the scope of Article 6(7) DMA.

While there may be good reasons for some of these denials, Apple should not be allowed to frustrate the objectives of the DMA through an excessively rigid reading of Article 6(7). Doing so would be to the detriment of consumers, who should be able to benefit from greater interoperability between the iOS and iPadOS platforms and third-party hardware and software, thanks to the DMA.

BEUC reiterates the importance for Apple, beyond granting legitimate interoperability requests and working on the corresponding technical solutions, to **put in place a user experience that is as frictionless as possible** for the consumers who want to activate interoperable devices.

51 European Commission, CASE DMA.100203 – Article 6(7) – Apple – iOS – SP – Features for Connected Physical Devices (19 March 2025, accessed on 27 Oct. 2026); and European Commission, CASE DMA.100204 SP - Apple - Article 6(7) – Process (19 March 2025, accessed on 27 Oct. 2026).

52 113 requests had been made since 20 May 2025, as of 27 August 2026.

4. ByteDance

4.1. Consent for use of personal data

The DMA's Article 5(2) requires gatekeepers to seek consent from consumers before:

1. Combining their personal data from first and third-party sources for ads purposes;
2. Combining their personal data from the gatekeeper's core platform service with any other service;
3. Using their personal data from the gatekeeper's core platform service in another service provided by the gatekeeper;
4. Signing them in to other gatekeeper services to combine their personal data.

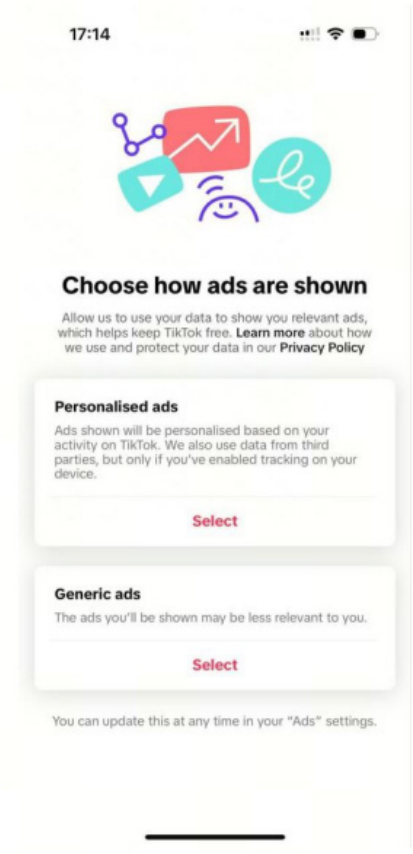
The DMA's recitals lay out further conditions, while Article 13 DMA prevents circumvention and consent must meet the criteria laid out in the GDPR.

ByteDance uses several mechanisms to seek consent from consumers to comply with Article 5(2) DMA. However, BEUC suspects these fail the compliance test.

First, in its various consent screens, ByteDance uses **non-neutral language,** which may be a breach of Article 13(6) DMA, and **behavioural techniques,** which breach Article 13(4) if they undermine effective compliance, to place the option it favours (consenting to more use/combination of personal data) in a positive light, while the alternative is portrayed negatively.

For instance, in the interface seeking consent for the combination of personal data from first and third-party sources for personal ads, ByteDance is pressuring consumers to provide their consent and is implying that, if they don't, it could lead to TikTok becoming a paying service (see figure 22).

Figure 22: user consent for first and third-party data for ads[53]

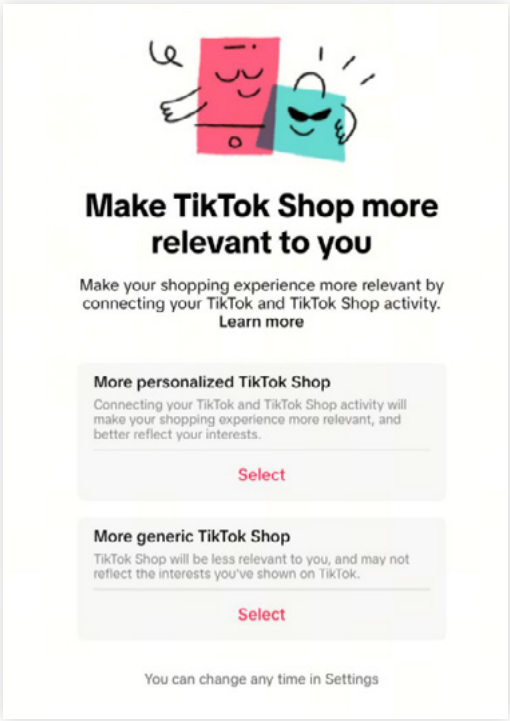


53 ByteDance, *DMA Compliance Report (Non-confidential Version)* (6 March 2026, accessed 2 September 2026), page 14.

ByteDance also limits the information provided for the "*Generic ads*" option to "*the ads you'll be shown may be less relevant to you.*" However, this only consists in providing negative information to the user and fails to highlight that less of the consumer's personal data will be used for ads purposes. This information is **neither balanced, nor objective.** Instead, ByteDance is employing a behavioural technique that leans heavily on loss aversion bias, where users are put off by options where they are told they will lose out.

ByteDance also uses non-neutral language and behavioural techniques when it seeks consent from consumers to use and/or combine their personal data across different services. In figure 23 below, which relates to consent for the combination of personal data across TikTok and TikTok Shop, the gatekeeper consistently and repeatedly refers to benefits if the user consents to the combination ("*make TikTok more relevant to you*"; "*make your shopping experience more relevant*"; "*Connecting your TikTok and TikTok Shop activity will make your shopping experience more relevant and better reflect your interests*"). In contrast, it only highlights negatives in the "*Generic ads*" option and there is no mention of the term "*personal data*", which is something consumers tend to want to protect, or that less of their personal data will be used for ads if the user selects this option.

Figure 23: choice screen for consent to combination of personal data between TikTok and TikTok Shop[54]

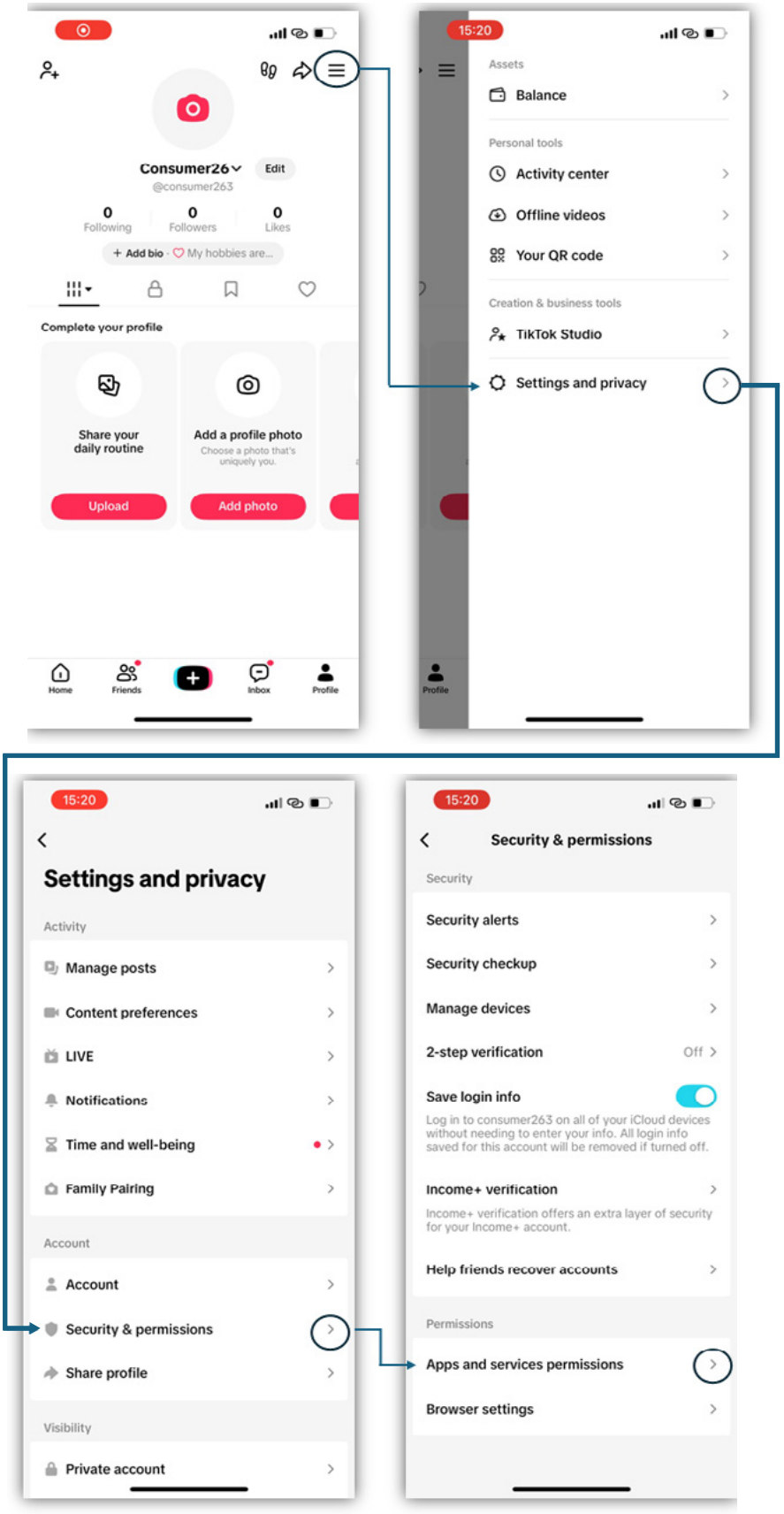


Secondly, ByteDance provides **vague and unclear information**. In the interface relating to the combination of personal data from first and third-party sources for ads (figure 23 above), ByteDance fails to explain what the "*generic ads*" option entails in terms of the consumer's personal data. While the compliance report is clearer in referring to personalised ads that do not involve the processing of personal data from third parties[55], the consent screen is inadequate in explaining this to the consumer. As a result, BEUC suspects consumers are unable to provide "*specific, informed and unambiguous consent*", as required under the GDPR.

Thirdly, ByteDance also makes the process for revoking previously granted consent **unnecessarily burdensome.** Where the consumer chooses to separate TikTok from TikTok Shop (see figure 24 and 25 below), finding the option to revoke consent in TikTok's settings is far from intuitive. The user must navigate at least eight separate steps, including multiple confirmation screens which continue to suggest reasons for keeping the cross-use/combination of personal data across the services activated without any indication as to why the user may want to keep them separate. The information provided is neither balanced nor objective, while the flow repeats some of the same steps and is designed to make it harder for the end user to revoke their consent than to give it.

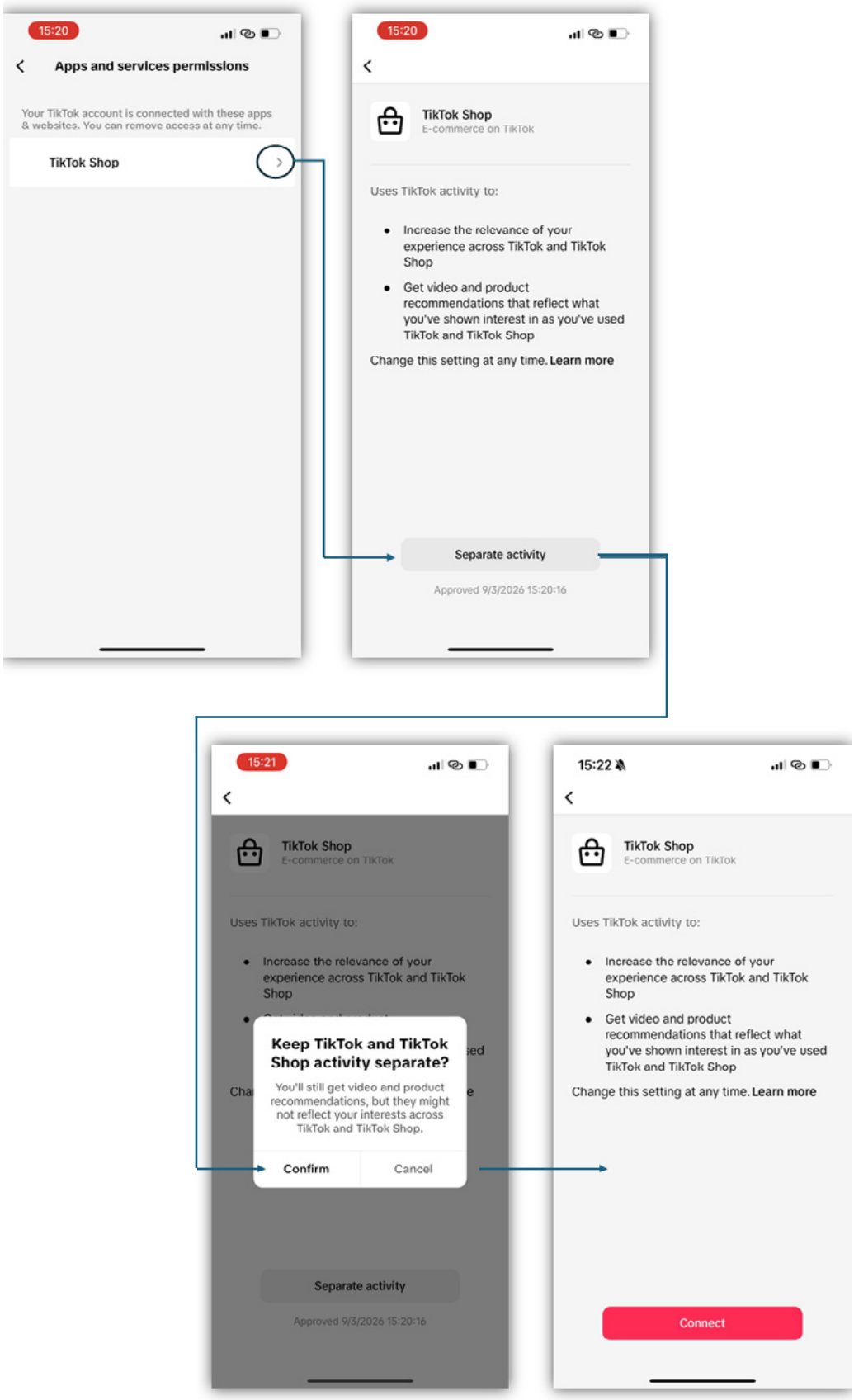
54 BEUC testing on iOS iPhone 16e device on 7 September 2026.
55 ByteDance, DMA Compliance Report (Non-confidential Version) (6 March 2026, accessed 2 September 2026), page 13, paragraph 11.

Figure 24: user flow to revoke consent for the combination of personal data between TikTok and TikTok Shop (steps 1-4)[56]



56 BEUC testing on iOS iPhone 16e on 3 September 2026.

Figure 25: user flow to revoke consent for the combination of personal data between TikTok and TikTok Shop (steps 5-8)[57]



57 BEUC testing on iPhone 16e on 3 September 2026.

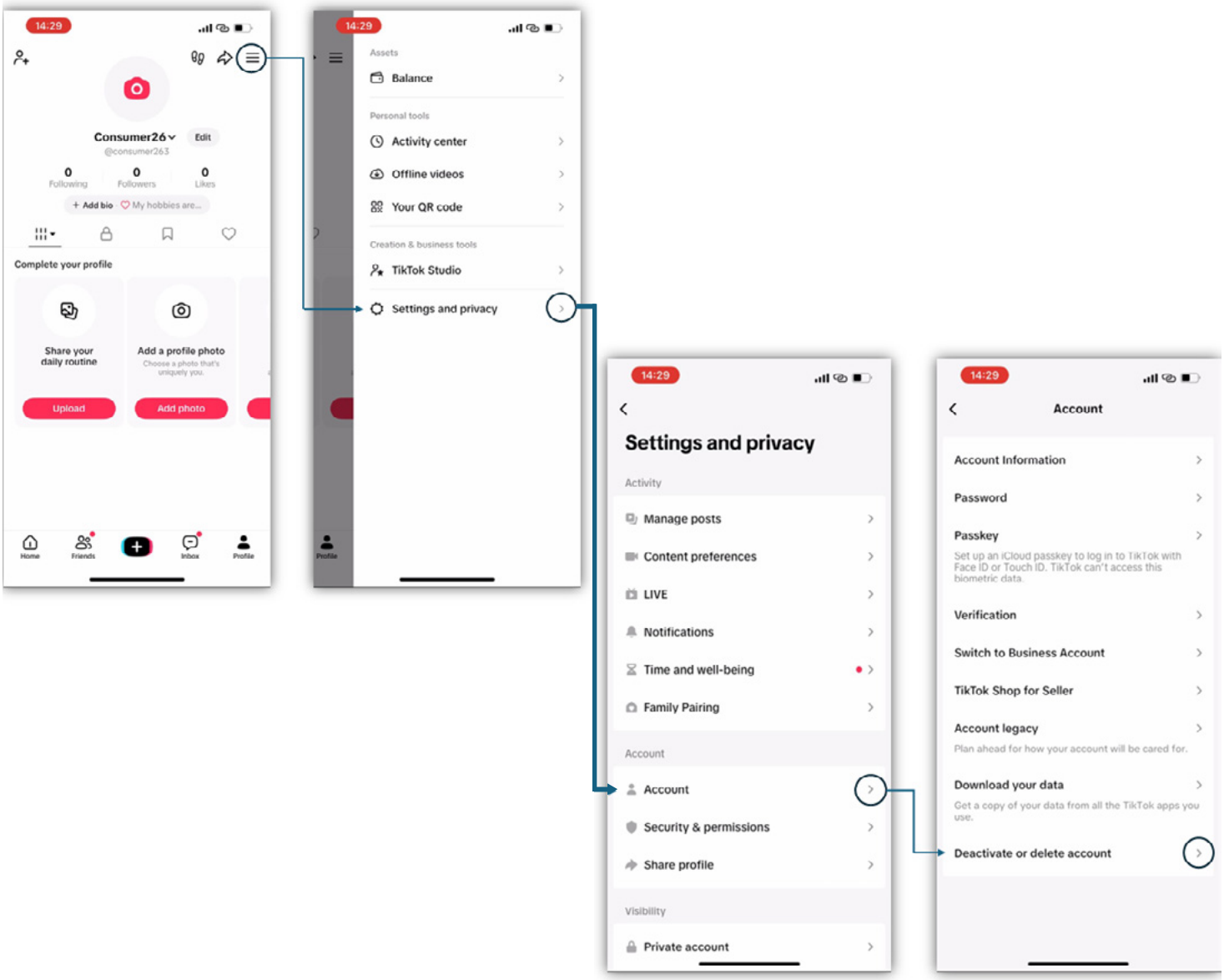
4.2. Termination of service

Gatekeepers must ensure it is possible to terminate a service without undue difficulty, according to Article 6(13) DMA, while the corresponding Recital 63 highlights that closing an account or unsubscribing should not be more complicated than opening one.

However, ByteDance's procedure for closing a TikTok account involves 9 screens and 11 steps (see figures 26 and 27 and 28). From the moment the user has found and clicked a first time on the option to close their account, the user effectively needs to carry out five different steps and confirm three times they want to close down their account, the equivalent of which does not happen when creating a TikTok account.

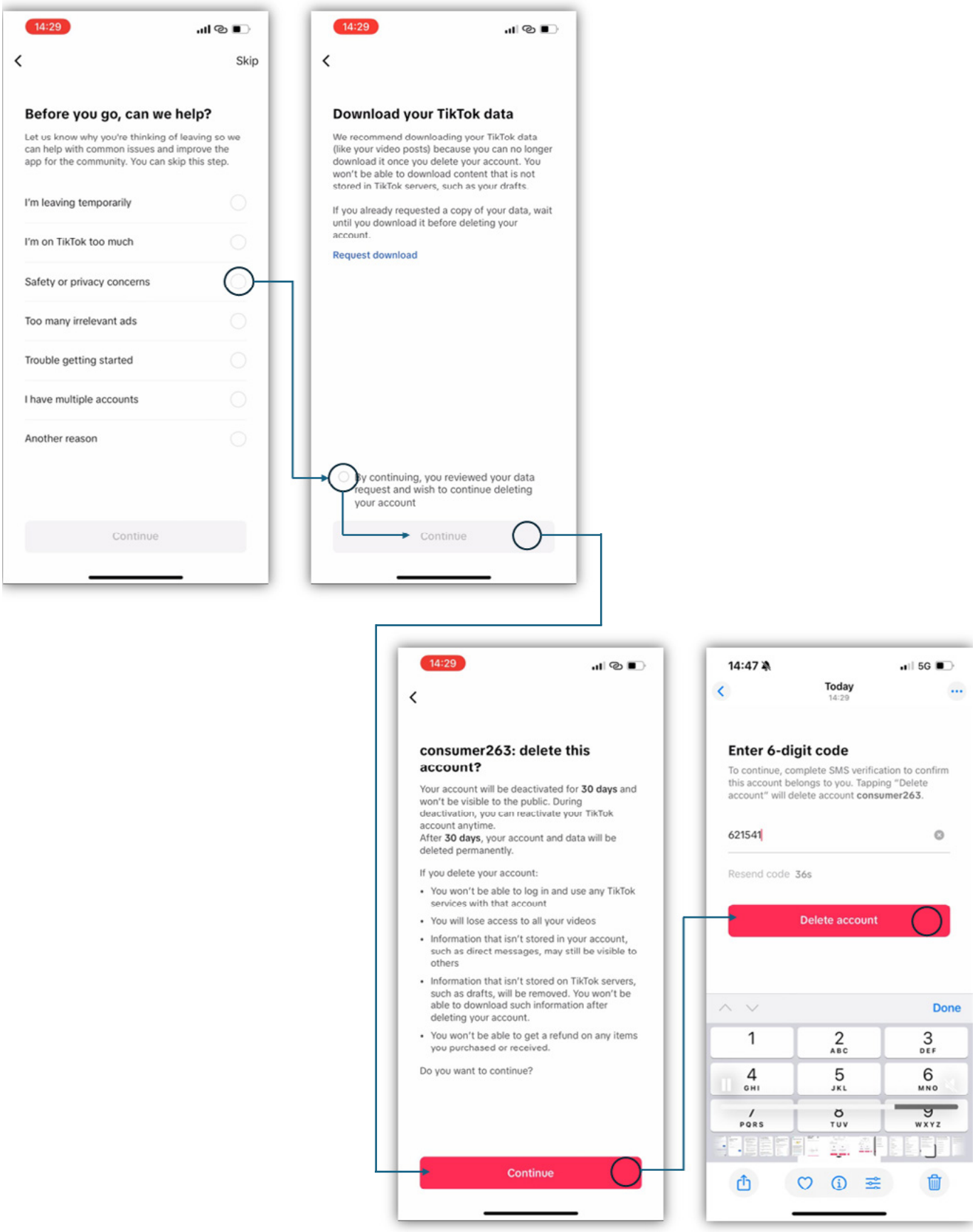
Such a process carries **undue difficulty** and constitutes a **flow that is more complex than the process of opening an account.** The interfaces are also designed in a way which very likely undermines effective compliance with Article 6(13). As a result, BEUC deems that this conduct breaches the DMA and ByteDance must amend its user flow in a way that is devoid of behavioural techniques and non-neutral interface design.

Figure 26: user flow to close down a user's TikTok account (steps 1-4)[58]



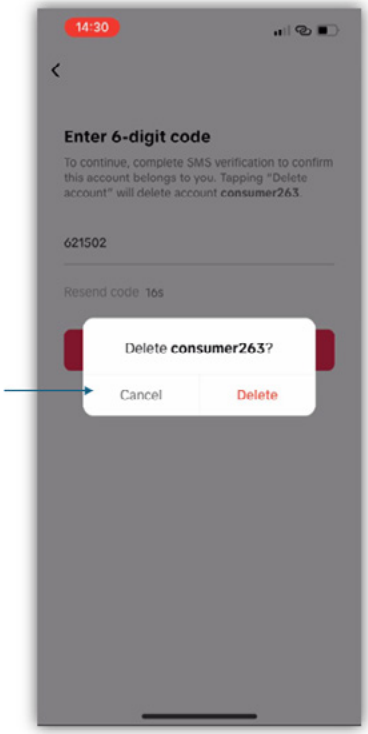
58 BEUC testing on iPhone 16e device on 3 September 2026.

Figure 27: steps 5-8 of the user flow to close down a user's TikTok account[59]



59 BEUC testing on iPhone 16e device on 3 September 2026.

Figure 28: step 9 of the user flow to close down a user's TikTok account[60]



60 BEUC testing on iPhone 16e device on 3 September 2026.

5. Meta

5.1. Consent for use of personal data

The DMA's Article 5(2) requires gatekeepers to seek consent from consumers before:

1. Combining their personal data from first and third-party sources for ads purposes;
2. Combining their personal data from the gatekeeper's core platform service with any other service;
3. Using their personal data from the gatekeeper's core platform service in another service provided by the gatekeeper;
4. Signing them in to other gatekeeper services to combine their personal data.

The DMA's recitals lay out further conditions, while Article 13 DMA prevents circumvention and consent must meet the criteria laid out in the GDPR.

Combining first and third-party sources of personal data for ads

To combine users' personal data from first and third-party sources for ads, Meta introduced a binary, pay-or-consent choice in November 2023. This triggered a Commission investigation which led to a Non-Compliance Decision in April 2025.[61] Meta has appealed this decision before the EU Courts (T-435/25) and BEUC will intervene as a third party in support of the Commission's decision.

Meta's latest changes, rolled out in January 2026 (see figure 29 and 30 below), however, have not solved non-compliance issues under the DMA and the GDPR.[62] BEUC has already carried out an analysis[63] about why it believes Meta's user flow continues to break the law.

Meta continues to use **non-neutral language and interface design techniques** in its user flow, undermining the free choice of users under the DMA. Meta also prevents users from providing free, specific, informed and unambiguous consent as required under the GDPR.

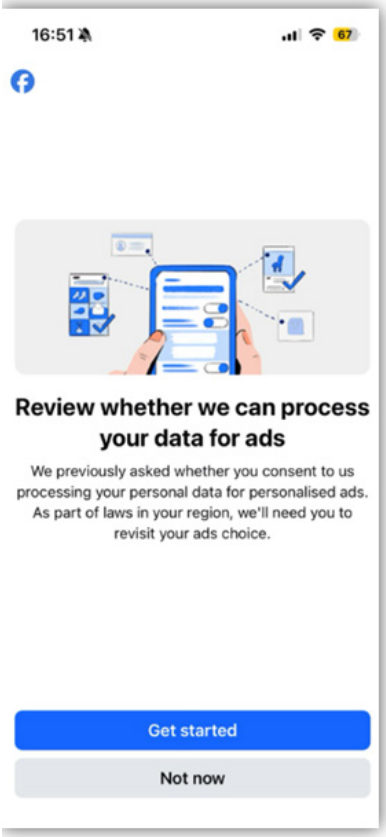
For instance, Meta does not provide the less personalised ads option (no combination of personal data from third parties with first party sources) on the same level as the options to pay not to see ads or the option to receive personalised ads. This makes it theoretically possible to **never reach the option to receive less personalised ads,** something the DMA expressly requires.

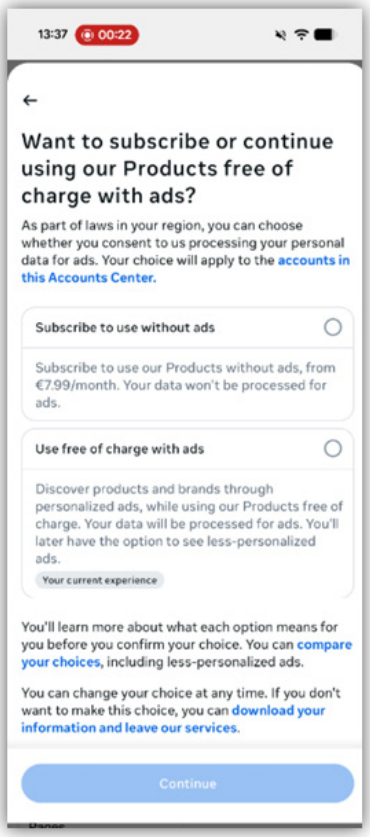
Users who select the "*less personalised ads*" option receive a **degraded experience**, which is forbidden under the DMA, because Meta imposes ad breaks on them. Meta cannot argue that ad breaks are necessary due to its inability to combine data from first and third-party sources.

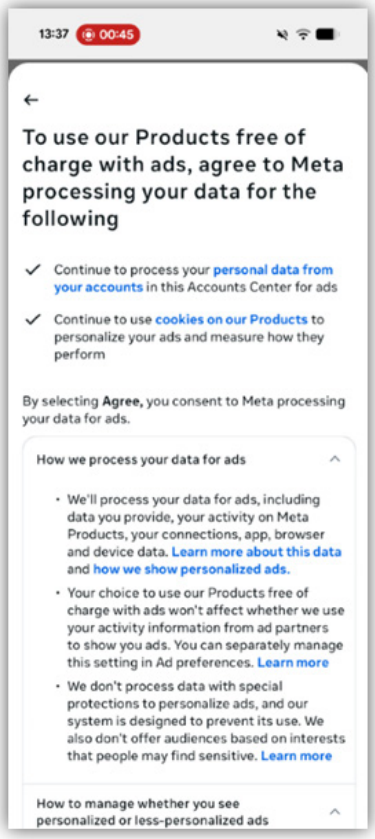
In addition, Meta describes the option to combine users' personal data from first and third-party sources in more positive terms than the alternative (see step 4 in figure 30 for example). The option to combine first party and third-party sources of personal data is also selected by default in that same step. This is a behavioural technique that plays on status quo bias, which is where users are more likely to stick to the status quo than to make a change.

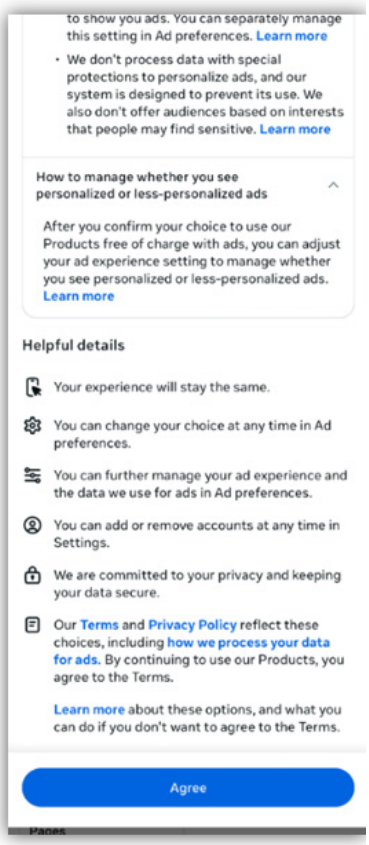
61 European Commission, Commission finds Apple and Meta in breach of the Digital Markets Act (23 April 2025, accessed 14 October 2026).
62 BEUC believes Meta is also breaching the Unfair Commercial Practices Directive (EU Directive 2005/29).
63 BEUC, Report: 'Users Still Stuck in the Mud: An Analysis of Meta's 2026 Changes to its Consent-for-Ads Mechanism against EU Law' (17 March 2026, accessed on 7 September 2026).

Figure 29: Steps 1-3 of Meta's consent-for-ads flow[64]



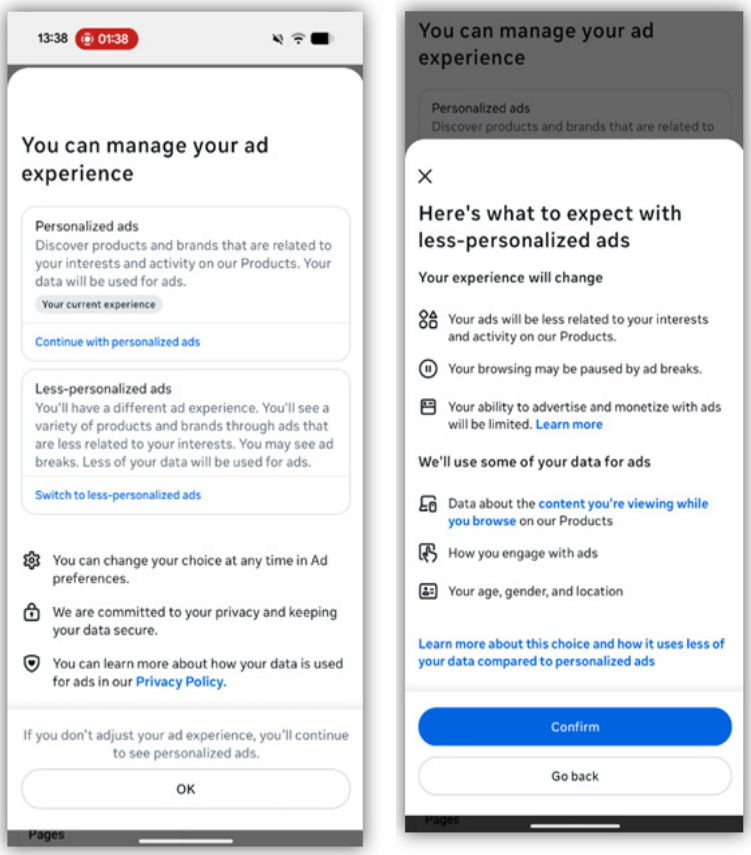






64 BEUC testing on Android Pixel 9a device on 28 January 2026.

Figure 30: Steps 4-5 of Meta's consent-for-ads flow[65]



To comply with the DMA, Meta must also comply with GDPR requirements around consent. This means it should minimise the data that it collects, with restrictions on the quantity, time and type of personal data collected and processed. Meta's description of its data collection does not appear to restrict the types of data it collects on its own platforms.

Meta must also allow informed consent, meaning that it must explain the data processing operations they are consenting to in order to provide ads. Yet Meta never informs the about what operations run in the background to provide the ads the consumer sees.

Cross-use/combination of personal data across different services

Meta uses different choice screens for each of the services for which it seeks consent to use and/or combine personal data with another service. For instance, it uses different consent screens between Facebook and Instagram, between Facebook and Messenger, between Facebook and Facebook Gaming, or between Facebook and Facebook Marketplace. However, all of Meta's consent screens use **non-neutral information, behavioural techniques and/or interface designs** which may have the effect of undermining its effective compliance with Article 5(2) of the DMA. BEUC will only highlight some examples here to avoid repetition.

For example, in the user flow to confirm the linking of the user's Facebook and Instagram accounts, Meta presents consumers with information that uses various elements of **non-neutral language** to describe the choice the end user is making (see figure 31). The description only highlights the positive aspect of *"unlocking features"* when combining accounts on the two services. This is **neither balanced nor objective** information, and therefore likely breaches Article 13(6) DMA, in BEUC's opinion.

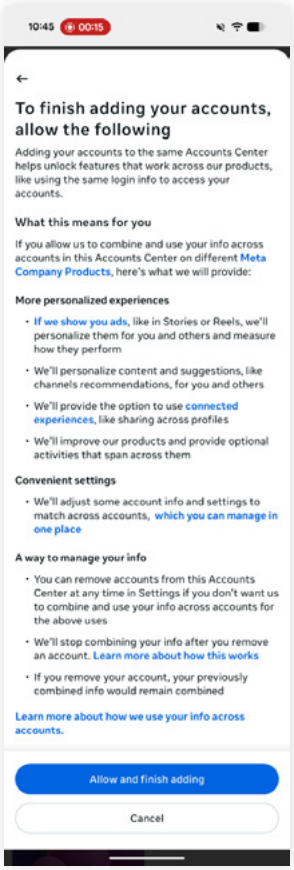
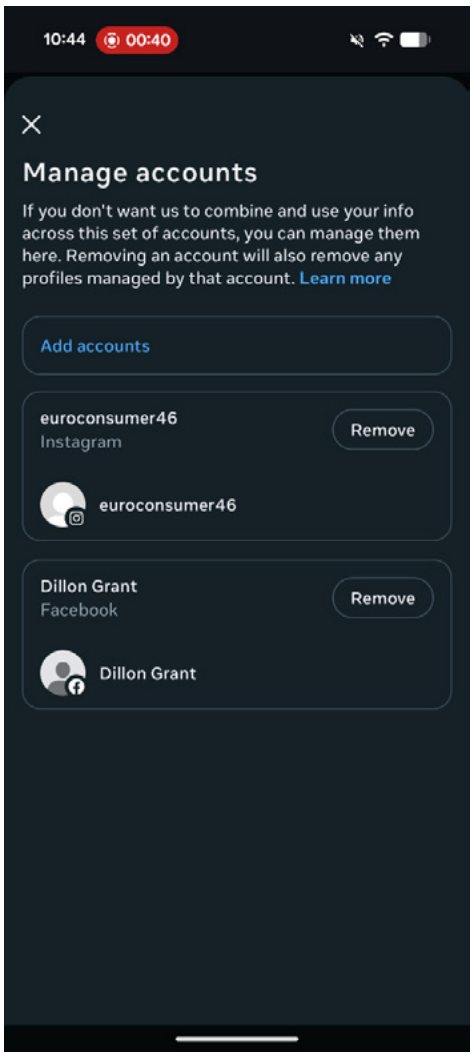


Figure 31: linking Facebook and Instagram to use/combine personal data across services[66]

65 BEUC testing on Android Pixel 9a device on 28 January 2026.
66 BEUC testing on Android Pixel 9a device on 18 December 2025 and rechecked on 16 July 2026.

The process to unlink the two accounts (six screens) is also **longer than the process to link them** (four screens). It is unclear why Meta makes the unlinking process longer than the linking process. In addition, Meta displays information (see figure 32) that may create the impression that the end user will **lose key functionalities** and **have their account closed** if they unlink their accounts (*"removing an account will also remove any profiles managed by that account*.") This could have the impact of pushing consumers to keep their accounts linked rather than to separate them. Subsequent screens continue to highlight features that the user will lose if they do not keep their accounts linked.

Figure 32: screen 3 of the user flow to unlink the end user's Facebook from Instagram account[67]

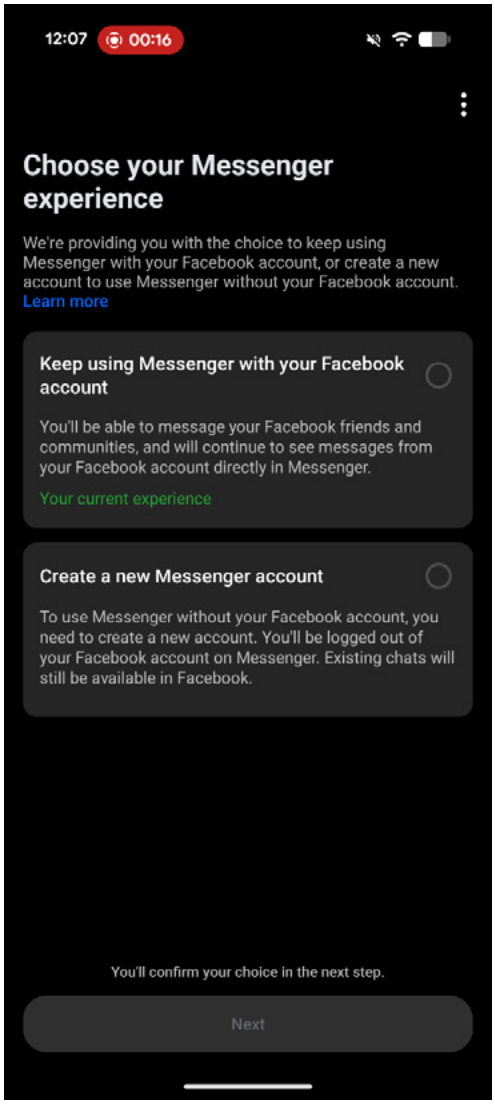


A clear example of **non-neutral interface design** comes from the Facebook-Messenger combination. By default, Meta provides Facebook with Messenger, which means the default is to use/combine data across the two services. Such an approach is favourable to Meta's interests, but not to the end users who might prefer not to have their personal data cross-used/combined across both services. In addition, it is possible to create a Messenger account without a Facebook account (see figure 33), so it is unclear why Meta cannot create a Facebook account without Messenger.

67 BEUC testing on Android Pixel 9a device on 18 December 2025 and checked again on 16 July 2026.

However, that the end user needs to unlink them after they have been provided together (see figure 33) can have negative implications in terms of **time and effort** because it requires the creation of a separate Messenger account. Here, Meta plays on **status quo bias** where users are more likely to stick to the status quo which requires less effort. The outcome, however, is that consumers are more likely to keep both services connected than separate. It also uses a green colour to highlight the status quo in order to make the option more salient to the consumer.

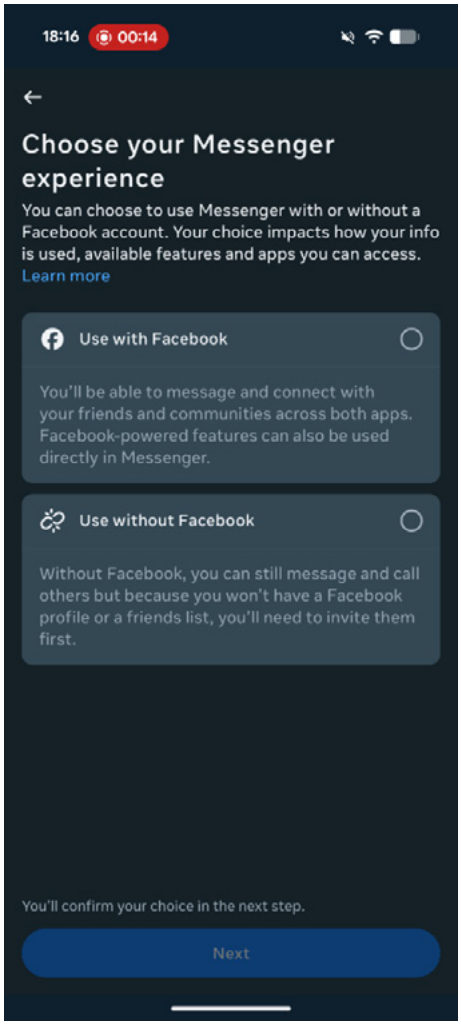
Figure 33: screen 2 of the user flow to keep Messenger linked to Facebook[68]



68 BEUC testing on Android Pixel 9a device on 13 January 2026 and checked on 16 July 2026.

When creating a standalone Messenger account, Meta uses non-neutral language to push users to create a Facebook account (see figure 34).

Figure 34: screen 3 of the user flow to create a Messenger account on mobile device[69]

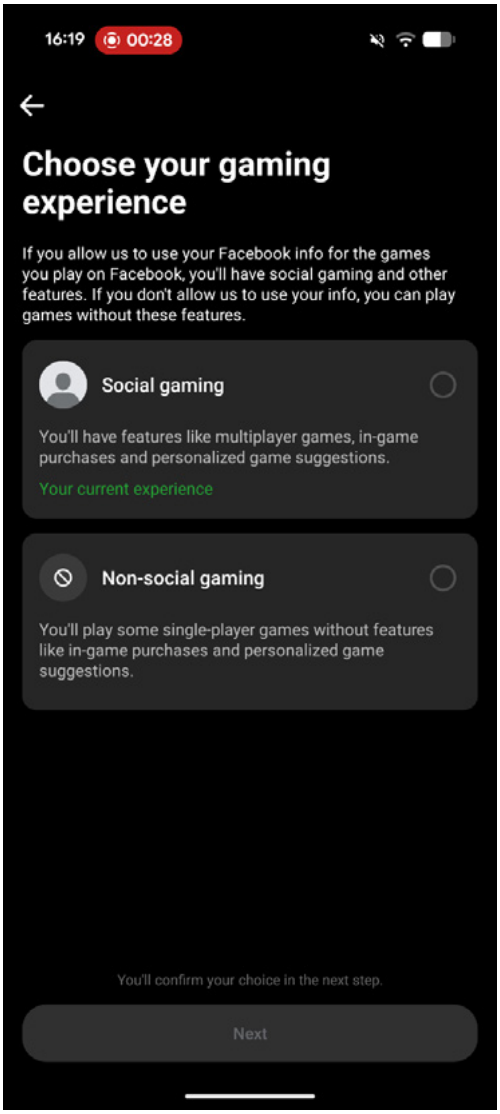


The description Meta provides under the "*Use with Facebook*" option appears to provide **only advantages** for the end user e.g. "*Facebook-powered features can also be used directly in Messenger*", while the option not to link Messenger to Facebook describes a **drawback** in having to first invite users before messaging them. How this constitutes a drawback is unclear, however, given that both a Facebook account and a standalone Messenger require the end user to first invite somebody before contacting them.

Meta also pushes consumers to consent to the cross-use/combination of their personal data between Facebook and Facebook Gaming (see figure 35). First, the default and status quo is that the personal data is used/combined across the two services, whereas Meta should be seeking consent ***before*** it cross-uses/combines the data in question. This allows Meta to lean on status quo bias and requires users to change the default, thus making it less likely to happen. Second, the default option is highlighted in green, which increases the saliency of the option that Meta prefers and increases the likelihood of it being selected. Finally, the option to keep the two services separate describes only disadvantages and a degraded experience, while the option to cross-use/combine the data is described only in positive terms ("*You'll play some single-player games without features like in-game purchases and personalised game suggestions*" VS "*You'll have features like multiplayer games, in-game purchases and personalised game suggestions*").

69 BEUC testing on Android Pixel 9a device on 13 January 2026 and cross-checked on 16 July 2026.

Figure 35: screen 2 of user flow informing end users about their choice regarding the cross-use/combination of their personal data between Facebook and Facebook Gaming[70]



Throughout its various interfaces, Meta repeatedly uses **non-neutral language, interface design and behavioural techniques.** These practices are likely to fall foul of Article 13 DMA, according to BEUC.

5.2. Tying

The DMA's Article 5(8) prevents gatekeepers from tying a core platform service to another core platform service, or to any other service which meets the DMA thresholds but is not designated as a core platform service. Article 13 DMA prevents any circumvention of this prohibition.

BEUC has concerns that Meta is undermining its effective compliance with Article 5(8) DMA and thus breaching Article 13(4) DMA.

When end users create a Facebook account for the first time, at no point during the account creation process do they receive a choice about whether they want to use Messenger with Facebook. This is despite Messenger being designated as a separate core platform service from Facebook under the DMA.

70 BEUC testing on Pixel 9a Android device on 19 December 2025 and checked again on 16 July 2026.

It is only after setup and use of the Facebook account, which includes Messenger, that Meta prompts end users to decide whether they want to continue using Facebook and Messenger together or to separate them. However, the design of the user flow in this manner has several implications for consumers.

First, maintaining the two services connected after setup requires no effort, while separating them **requires both action and effort from the user**. The latter requires the creation of a separate Messenger account, with a separate username, which is time-consuming. This approach leans heavily **on status quo bias**, which is a well-known cognitive bias that humans have in which they prefer the status quo over change, particularly if the change requires effort.

Secondly, untying the two services can cause detriment if the user has begun to use Messenger based on their list of contacts on Facebook and then loses access to their list of contacts because the creation of a separate Messenger account requires the manual repopulation of their contact list in Messenger.

Initially, end users are required to use both services, as there is no option to use Facebook without Messenger which is a questionable structure for the interface design.

This questionable structure is compounded by the fact that, as already described in section 5.1 above, Meta provides a different user flow when users are trying to create a Messenger account. Here, Meta presents users, as part of the installation process, with the option to create a Facebook account that is linked to their Messenger account. Furthermore, in the user flow, Meta displays non-neutral language to push consumers to create a Facebook account in addition to their Messenger account (as described in section 5.1 above).

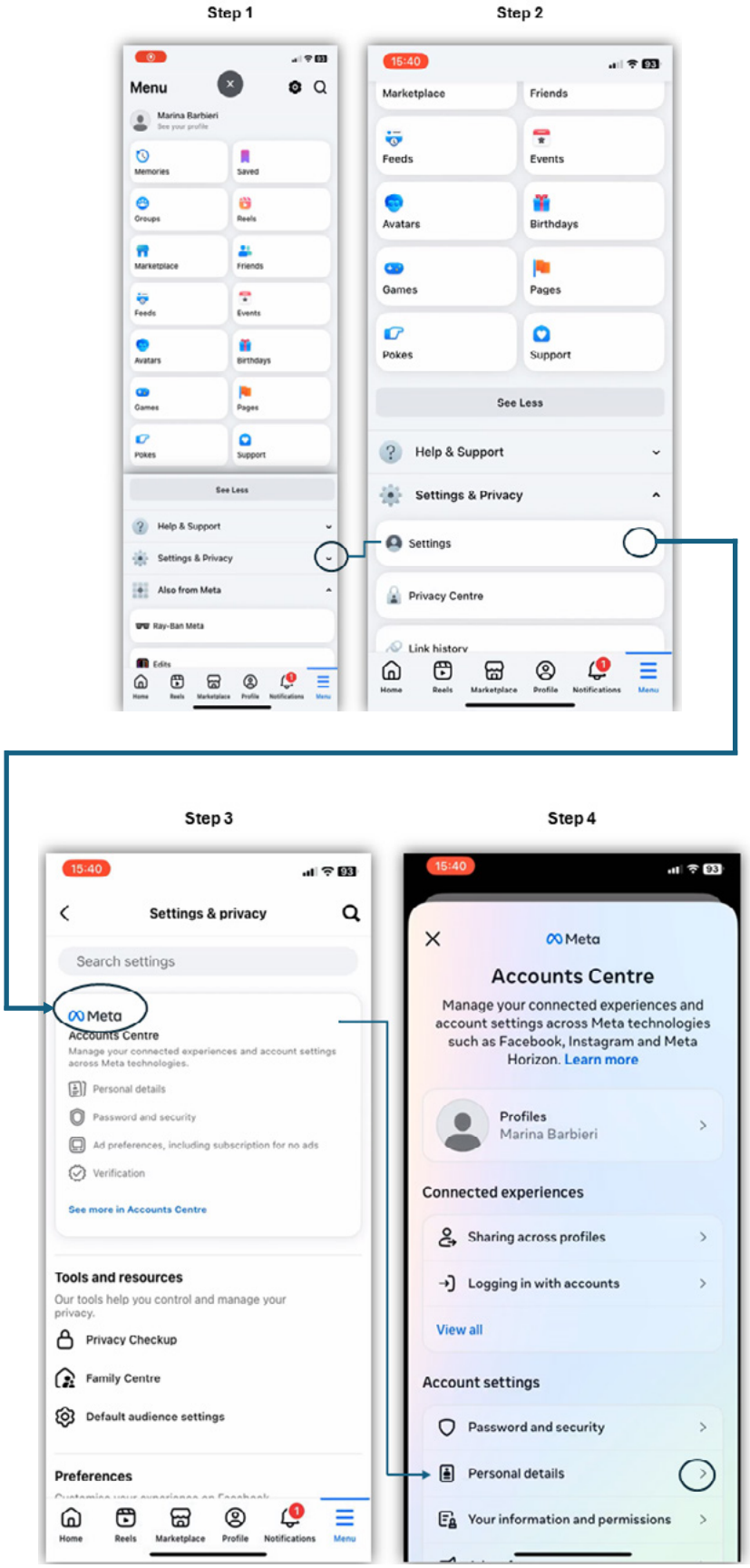
5.3. Termination of service

Gatekeepers must ensure it is possible to terminate a service without undue difficulty, according to Article 6(13) DMA, while the corresponding Recital 63 highlights that closing an account or unsubscribing should not be more complicated than opening one.

However, Meta makes unsubscribing from either Facebook or Instagram a **non-intuitive and unnecessarily long sequence of steps.** There are sixteen steps in total. In contrast, creating an account on either of these platforms is a straightforward and intuitive process, with clearly defined steps that allow users to successfully register.

The screenshots presented below relate to the deletion of a Facebook account, but the procedure for the permanent deletion of an Instagram account is identical and gives rise to the same issues.

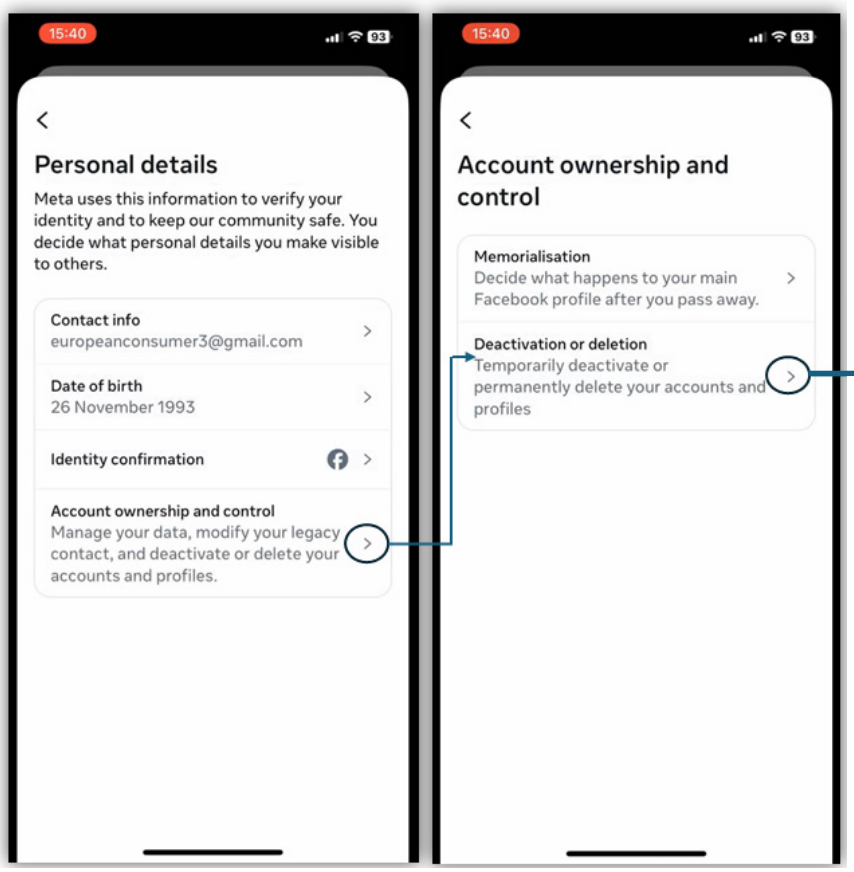
Figure 36: steps 1-16 in user flow to terminate a Facebook subscription[71]



71 BEUC testing on Android Pixel 9a device on 1 December 2025 and cross-checked on 16 July 2026.

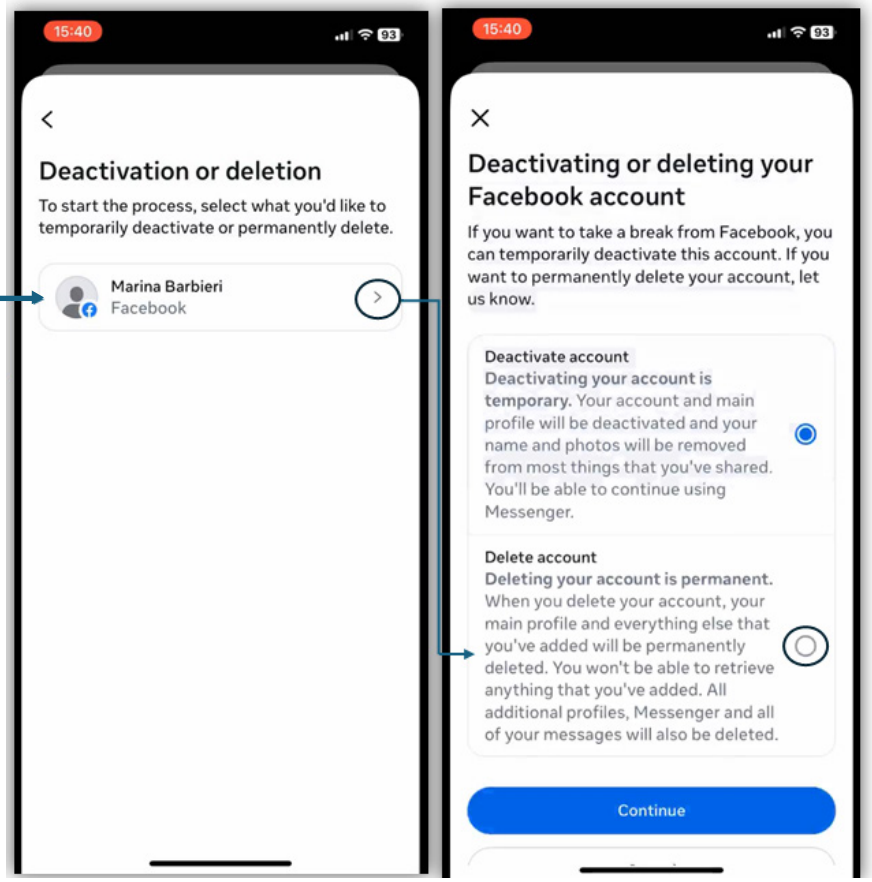
Step 5

Step 6

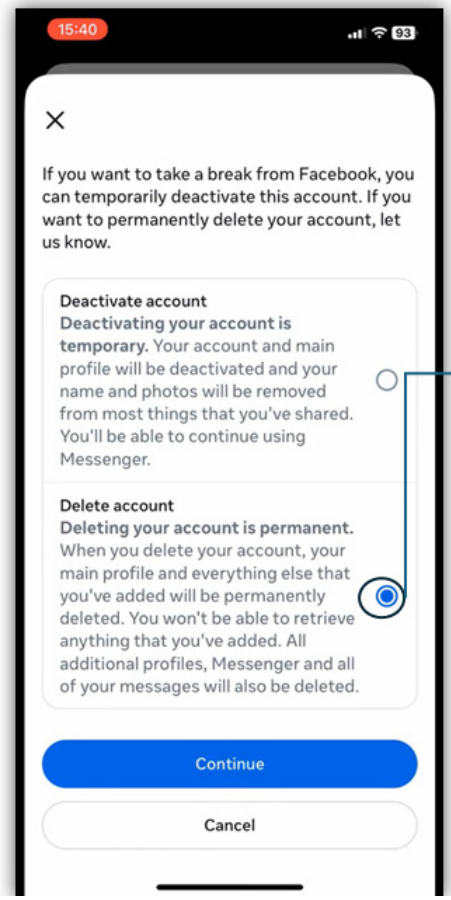


Step 7

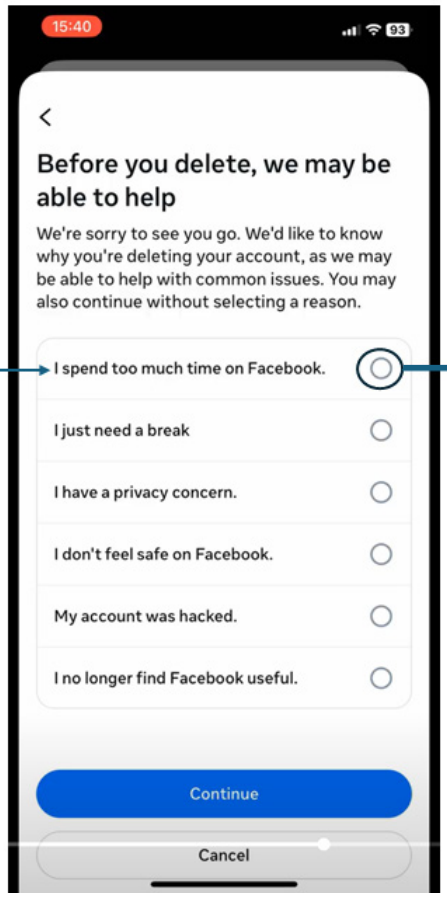
Step 8



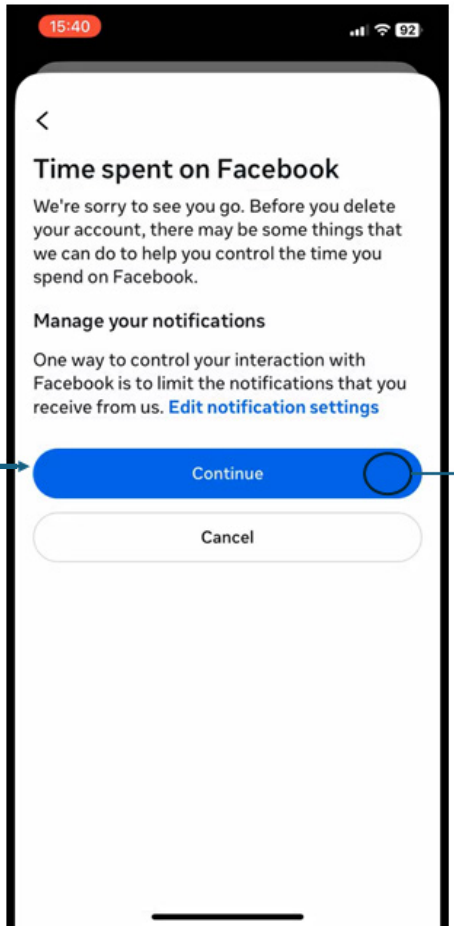
Step 9



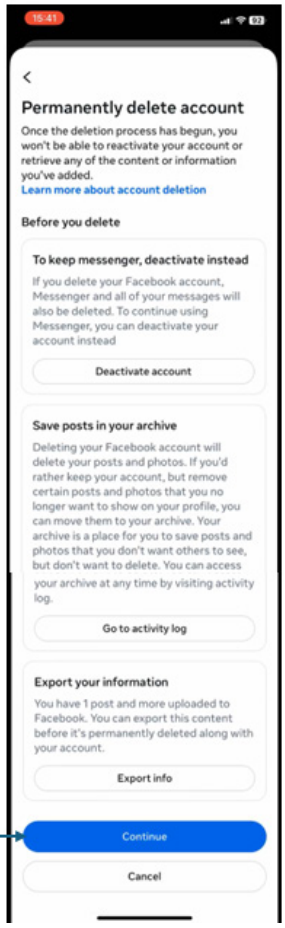
Step 10



Step 11

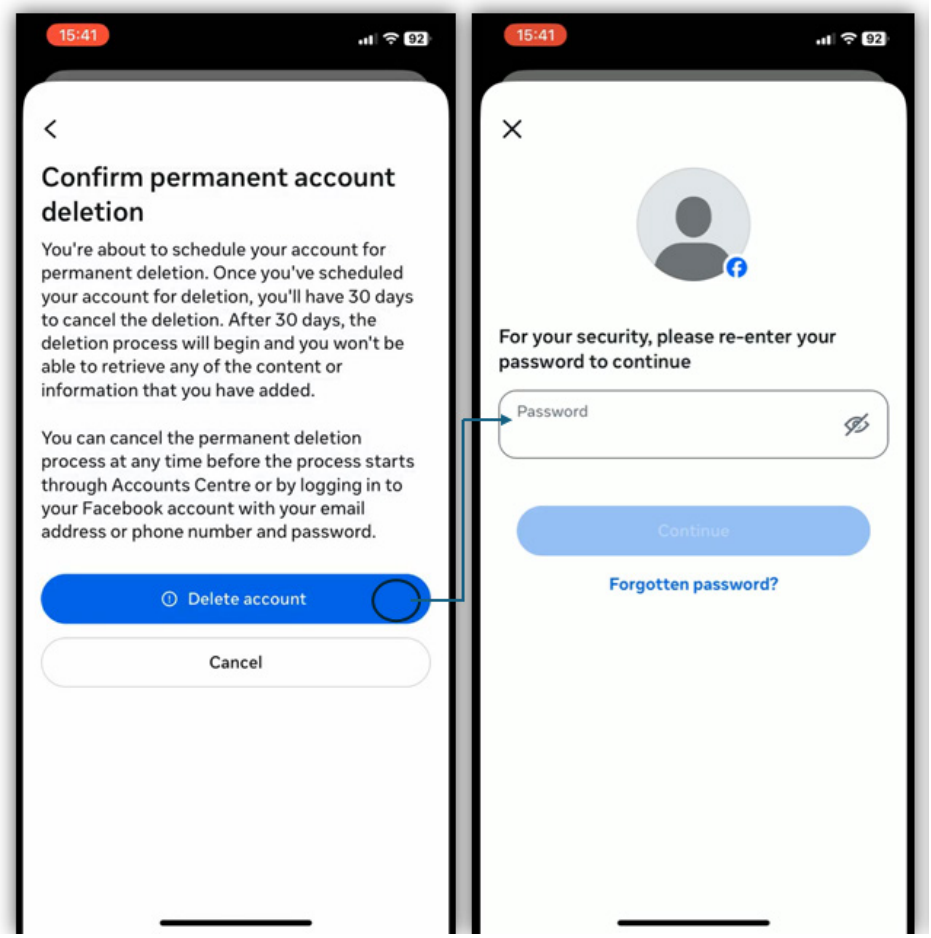


Step 12



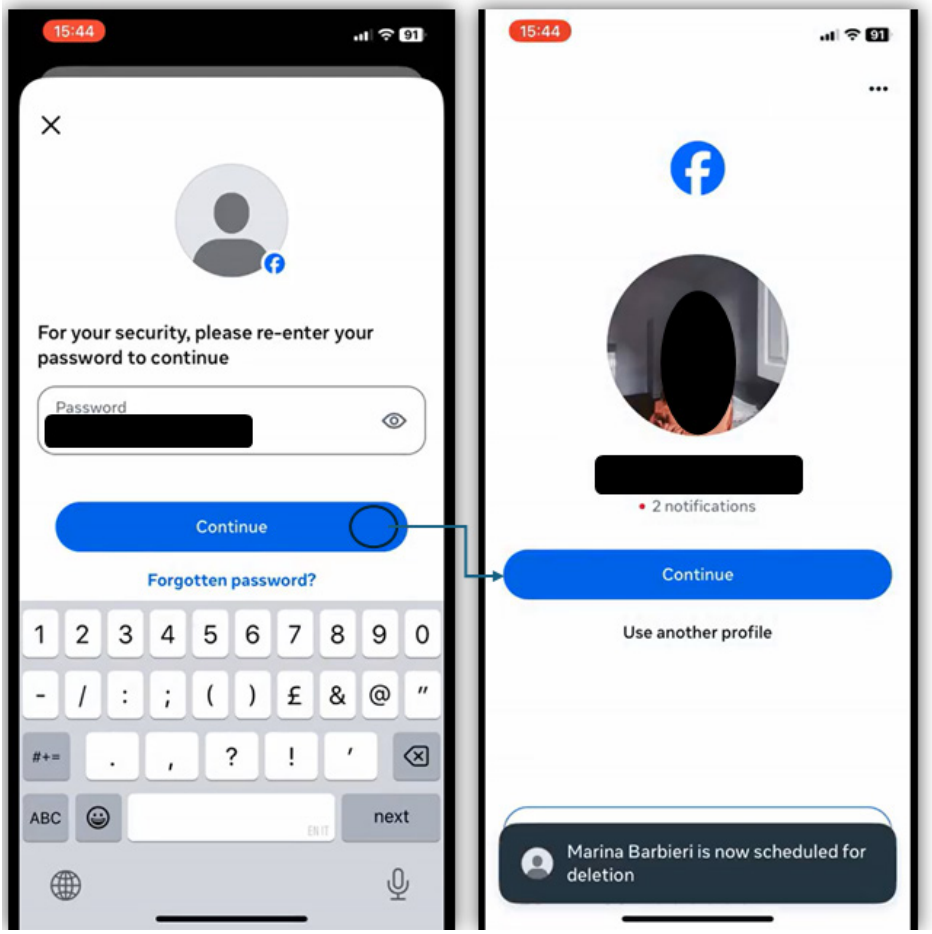
Step 13

Step 14



Step 15

Step 16



6. Microsoft

6.1. Consent for use of personal data

The DMA's Article 5(2) requires gatekeepers to seek consent from consumers before:

1. Combining their personal data from first and third-party sources for ads purposes;
2. Combining their personal data from the gatekeeper's core platform service with any other service;
3. Using their personal data from the gatekeeper's core platform service in another service provided by the gatekeeper;
4. Signing them in to other gatekeeper services to combine their personal data.

The DMA's recitals lay out further conditions, while Article 13 DMA prevents circumvention and consent must meet the criteria laid out in the GDPR.

Microsoft uses different interfaces to obtain consent from users to combine or use their data across different services. However, several of them use **behavioural techniques and non-neutral language** which may breach the DMA.

For example, the interface to cross-use/combine personal data between LinkedIn and other Microsoft services (see figure 37) leans heavily on **status quo bias**. The description uses terms such as *"keep your LinkedIn services connected"* implying that the default is that these services are connected. Yet there is no reason for this to be the case, especially if the user is opening a LinkedIn account for the first time. However, users tend to have a preference for the status quo over change, which may make users more inclined to connect the different services over separating them.

Microsoft describes the option to cross-use/combine the user's personal data across different services in only positive terms, such as *"We've always connected your LinkedIn experiences with our services to better tailor what you see"* or *"find jobs with better recommendations"* or *"build your skills with better course recommendations"* without any mention of drawbacks or description of what happens if the user does not consent.

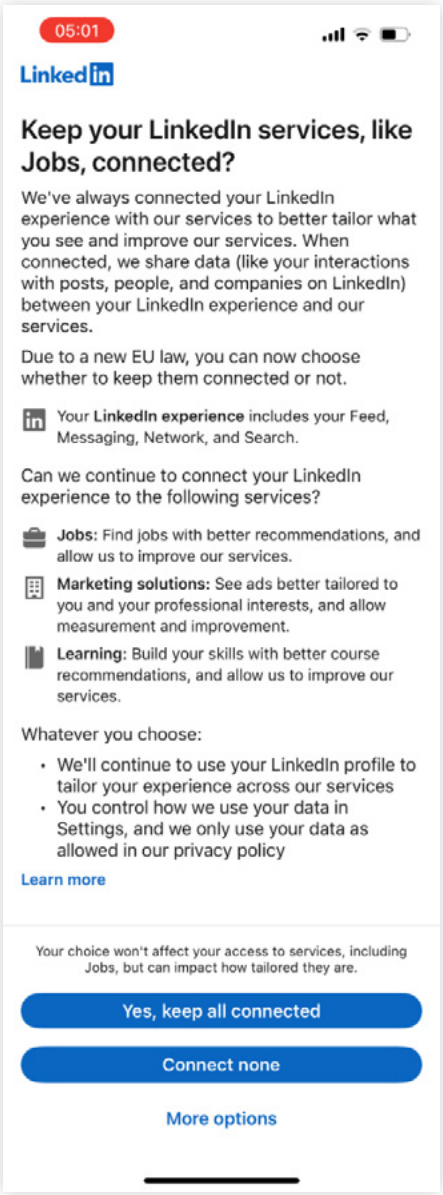
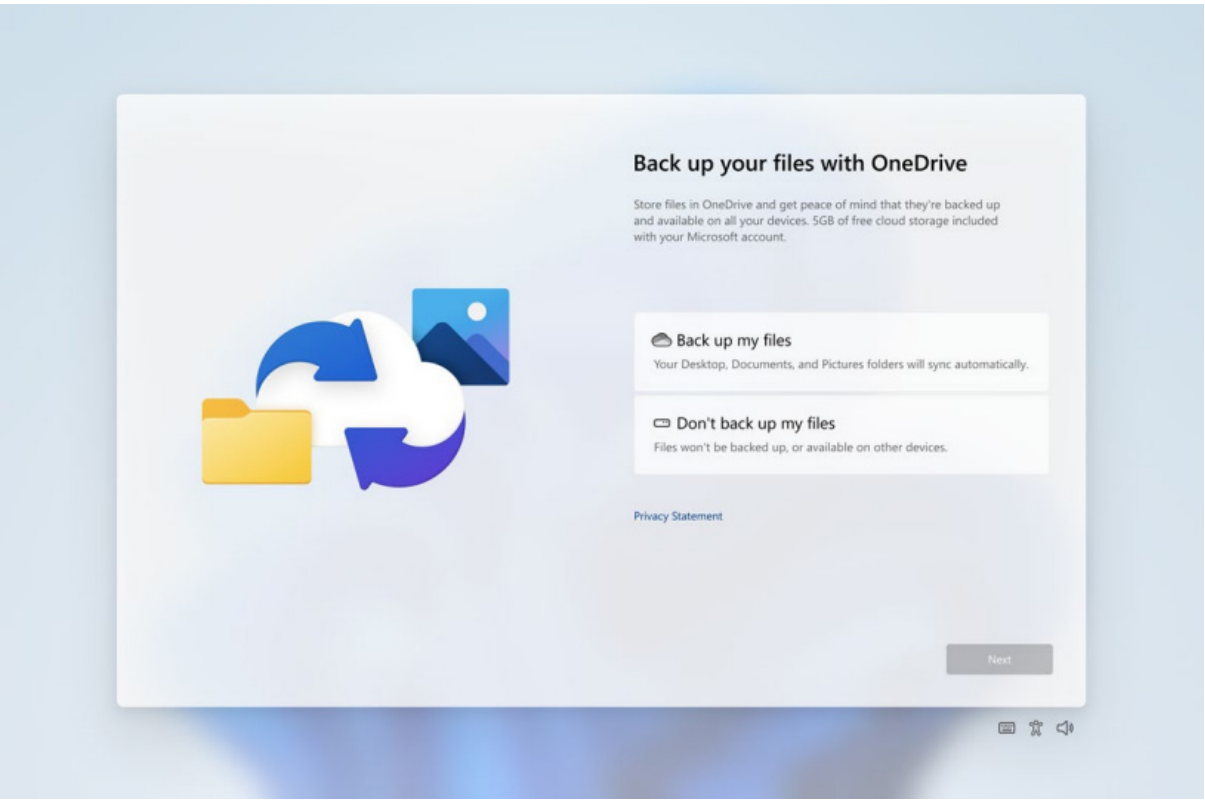


Figure 37: Screen 1 of user flow seeking consent for use of personal data between LinkedIn and other services[72]

72 BEUC testing on iOS iPhone 16e on 22 April 2026.

Another example of a behavioural technique Microsoft uses comes from the interface where it seeks consent to synchronise the personal data on a Windows device with personal data on OneDrive (see figure 38). Here, Microsoft leans heavily on **loss aversion bias** when it mentions that files won't *"be backed [up] or available on other devices"* in case they decline, implying that end users will **lose out** and be at **greater risk of losing their files**. In reality, end users can simply choose alternative cloud storage options belonging to third-party business users which could be just as safe an option.

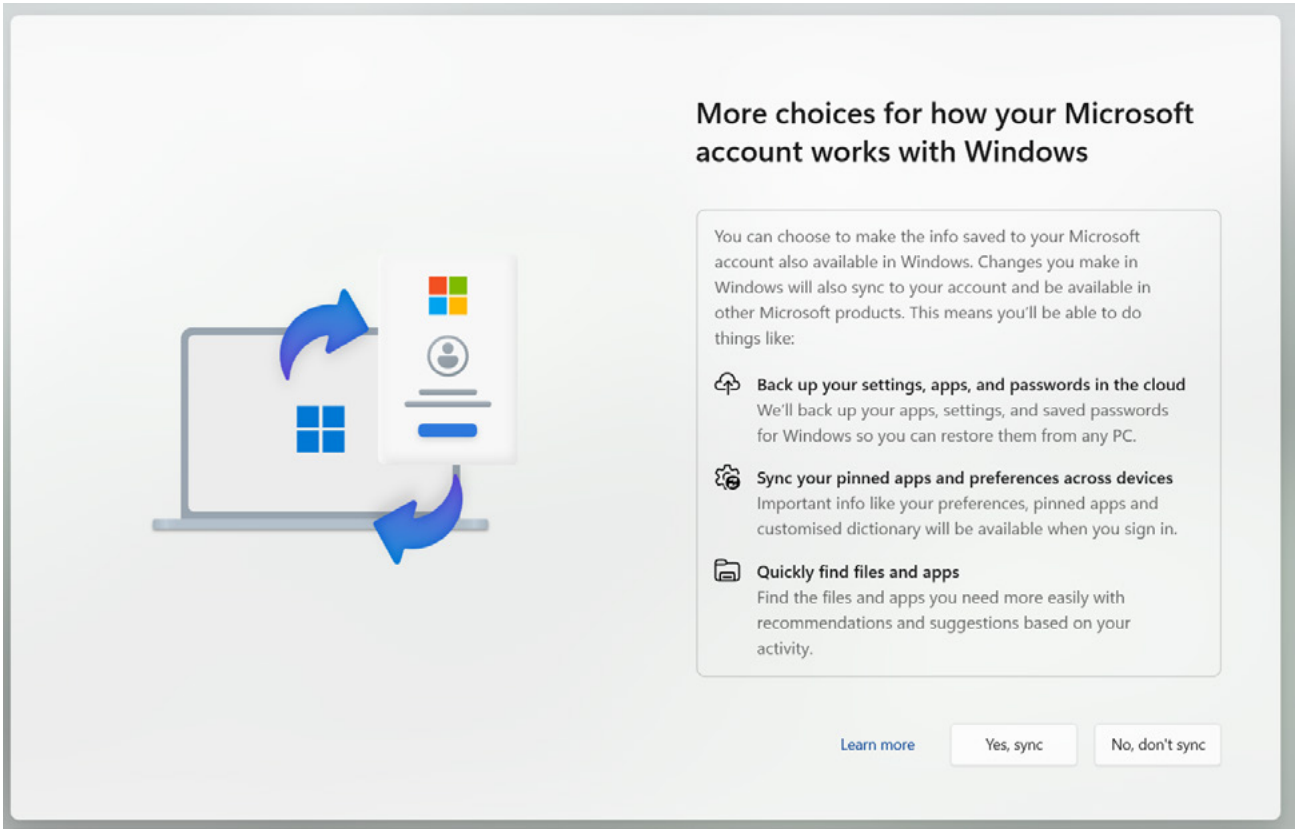
Figure 38: consent screen to share Windows data with OneDrive[73]



73 Microsoft, *Compliance Report – Annex 10 – Windows* (6 March 2026, accessed on 15 September 2026), p. 21.

A further use of **non-neutral language** to steer consumers to share more data comes from the interface to synchronise personal data from Windows with the Microsoft Account (see figure 39 below). Microsoft describes in only positive terms what happens if the user consents to the use/combination of their data across services.

Figure 39: consent screen to synchronise data between Windows and the Microsoft Account[74]

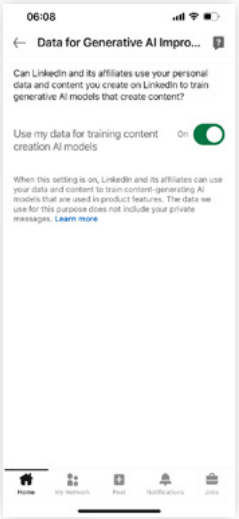


One notable exception to the trend mentioned above is **LinkedIn's consent screen for ads purposes**, which is a good example of how gatekeepers are able to design more neutral interfaces when they try. Microsoft does not use any obvious non-neutral language, interface design or behavioural techniques and other gatekeepers could find inspiration in this type of interface in it.

74 BEUC testing on HP Windows-operated desktop on 2 May 2026.

One area where Microsoft does not currently seek consent, but potentially should, is in using consumers' personal data on LinkedIn to train generative AI models that create content. Currently, the toggle is on by default (see figure 40).

Figure 40: screenshot in LinkedIn settings regarding whether LinkedIn personal data can be used to train generative AI models[75]



Since AI models are likely to end up being used in services at a later stage, and that obtaining consent from consumers at that stage is impossible once the model has been trained on their data, it would make sense that LinkedIn seeks consent on the basis of Article 5(2)b) from consumers ***before*** using their personal data. This specific use should be made clear to end users in the consent screens such as in figure 40 above and the toggle should be turned off by default as a result.

6.2. Uninstalling and setting alternative apps as defaults

Gatekeepers must allow consumers to easily uninstall apps and change default settings that steer them to using the gatekeeper's apps under Article 6(3) DMA. The latter includes prompting consumers to select the browser, search engine or virtual assistant of their choice as the default across the gatekeeper's designated service. The DMA's recitals lay out further conditions, while Article 13 DMA prevents circumvention.

While Microsoft is not required to display a choice screen on Windows devices to allow the user to select their default search engine or browser, since neither Edge nor Bing have been designated as core platform services, Microsoft is nevertheless **bound to respect the choices made by users** regarding their defaults on Windows.

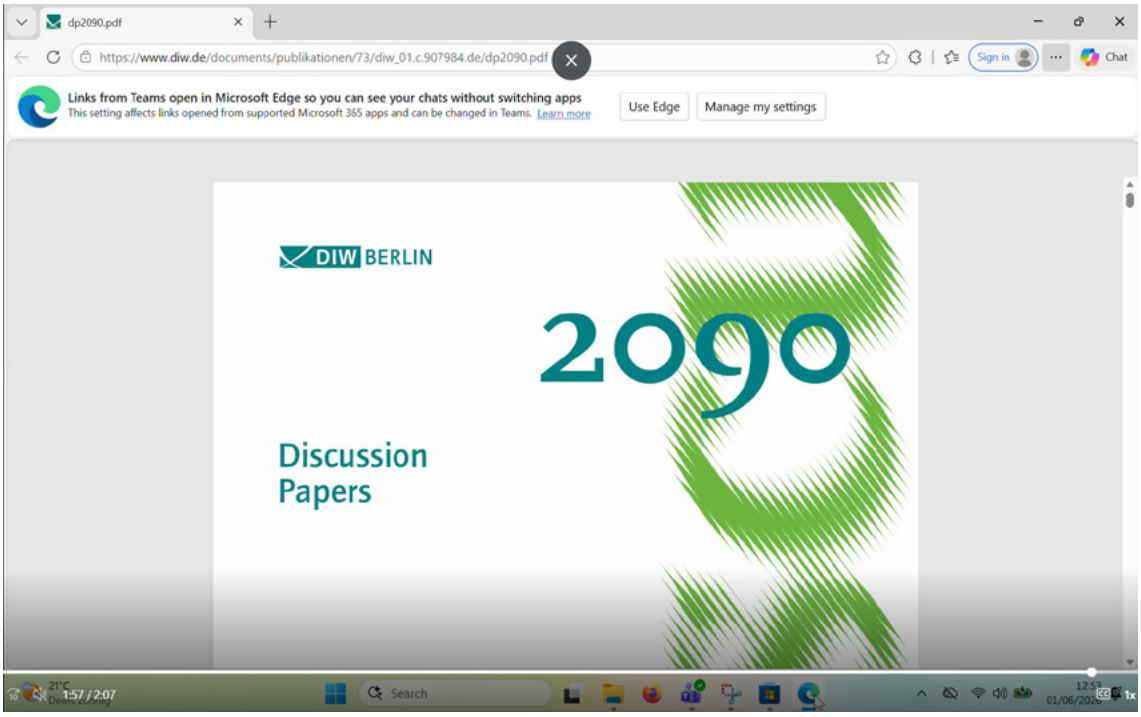
There are several problems with Microsoft's conduct, however, which undermine the choices made by the user:

1. **default opening of links from Microsoft apps in Edge**, even though a third-party browser has already been selected as default;
2. **no ability to easily change the default search engine** across Windows, and Bing is used unfairly in certain scenarios to disadvantage other search engines;
3. **repeated prompts in Windows** for the end user to switch to either Edge or Bing as their default;

First, even though an end user has already selected a third-party business user's browser as the default on Windows, certain Microsoft apps, such as Teams, **continue to steer end users to Edge**. When an end user clicks on a link in Teams, s/he has the link opened in Edge, rather than the browser already selected as default, as seen below in figure 41, unless Edge is uninstalled or the end user specifies in Windows settings that links from Teams should be opened in the default browser. BEUC considers this approach to be **unnecessarily complex and to undermine the ability of consumers to easily change their default settings.** It is, for example, significantly worse an experience than on iOS.

75 BEUC testing on iPhone 16e on 22 April 2026.

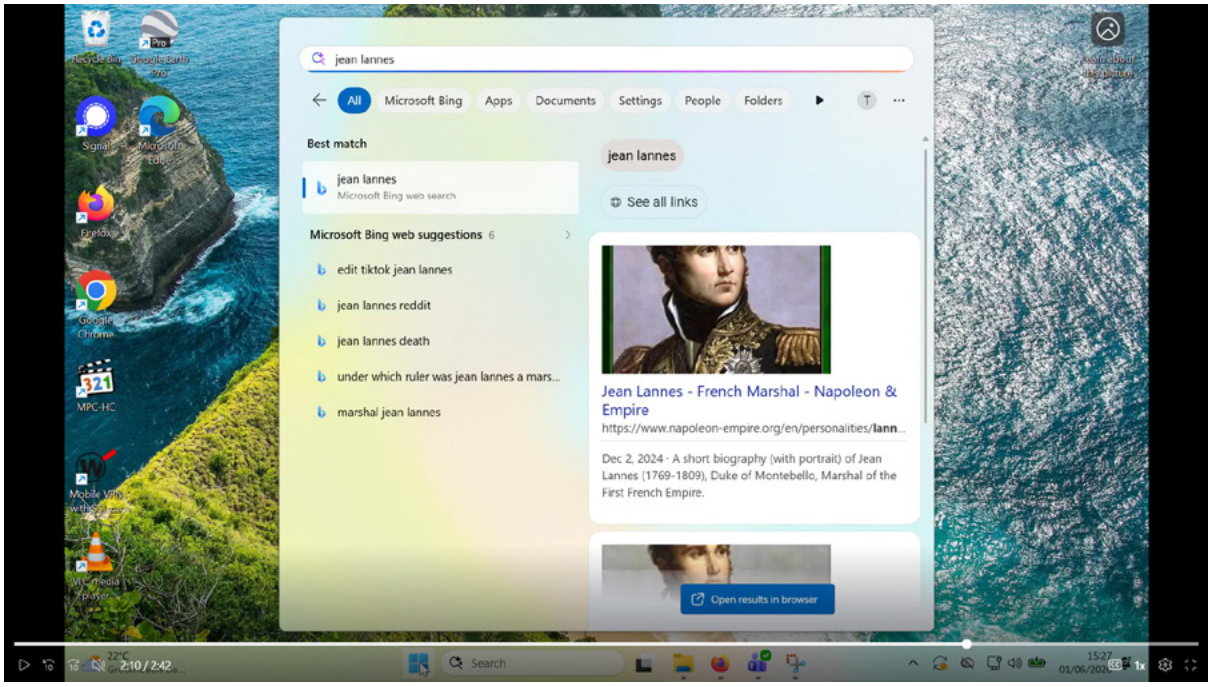
Figure 41: default opening of links from Microsoft Teams in Edge despite alternative browser set as default[76]



Secondly, Microsoft does not appear to give end users the ability to **set their default search engine across Windows and for all access points.** This practice is in contrast to the approach taken by other gatekeepers, such as Apple and Alphabet, and from Microsoft's own practice regarding browsers. It also means that it is easier for Microsoft to steer end users to Bing in certain conditions.

For example, unless Bing is uninstalled from Windows, end users will have Bing search results displayed when using the Windows Search function (see figure 42 below) regardless of the search engine set as default in their browser.

Figure 42: display of Bing search results when using Windows Search[77]



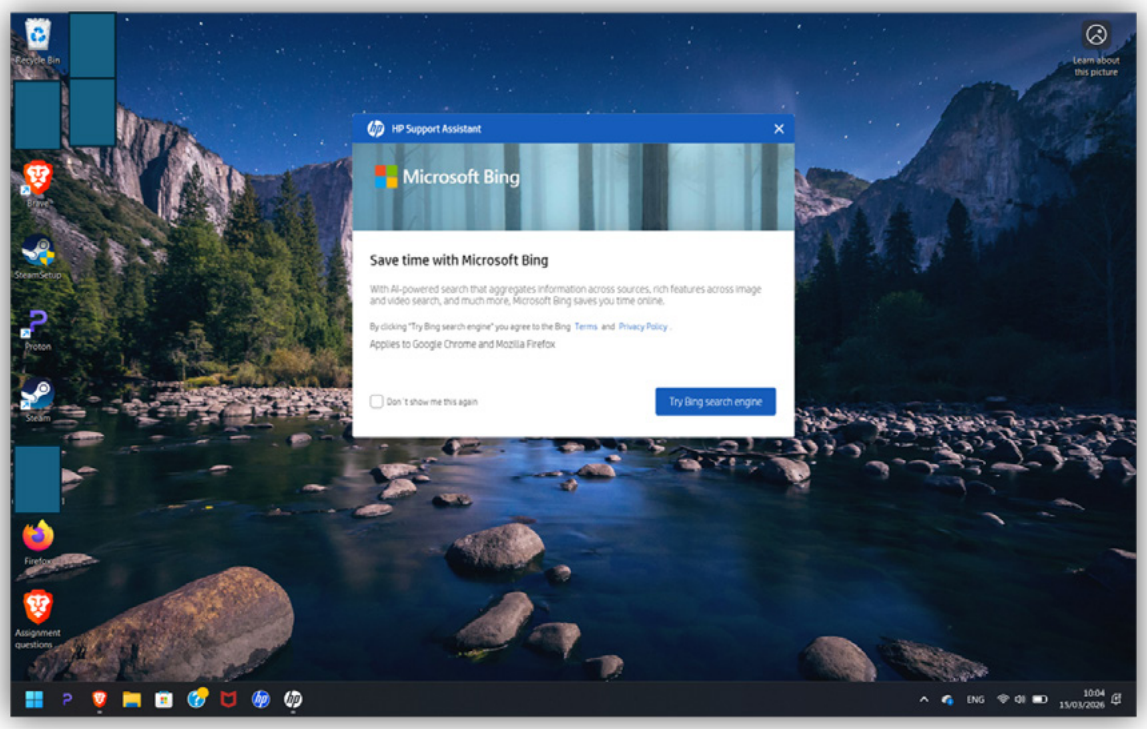
76 BEUC testing on HP desktop with Firefox set as default browser on 1 June 2026.
77 BEUC testing of Windows Search results on HP desktop on 02 June 2026.

It is only if users uninstall Bing from Windows that Windows Search does not display any Bing search results. However, Windows Search does not appear to display any search engine results in that case and it is difficult not to see this as a **degradation of the service**, which is prohibited under Article 13(6) DMA.

Third, Microsoft continues to **periodically prompt Windows users** who have already selected an alternative default browser or search engine to **switch back to Edge or Bing**. Microsoft also appears to be using increasingly subliminal techniques.

For example, figure 43 below was displayed to an end user on a Windows device, who had selected DuckDuckGo as their default search engine previously, in what appears to be a prompt from the device manufacturer (HP). It is Microsoft, however, that is likely to have required this prompt to be displayed to end users as part of an agreement with HP, given that Bing is a Microsoft, and not an HP, product.

Figure 43: prompt to switch default search engine on Windows to Bing[78]



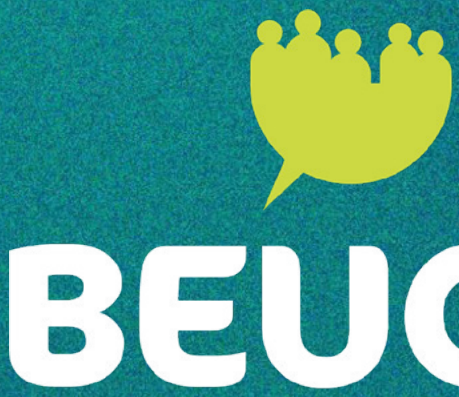
Given that these prompts are only displayed once an end user has selected an alternative search engine, their intent can only be to return the end user to the pre-installed and default search engine on Windows which is Bing. In effect, these prompts undermine the ability of end users to easily change default settings relating to search engines/browsers on Windows.

Finally, a question mark hangs over Microsoft's compliance relating to **S-Mode**, which Microsoft announced in 2025 it was discontinuing. S-Mode is a safety mode on Windows where the apps used come from the Microsoft Store and Edge is the default browser. This would solve many concerns that BEUC and other stakeholders have voiced about the compatibility of S-Mode with the DMA.

However, there is little information and clarity on when and **how this phase-out is taking place**. It is also unclear if such a phase-out only affects new Windows devices or will also apply to existing Windows devices. This matters substantially, as it could mean that Windows-users in S-Mode are deprived of their right to easily change default settings on their operating system regarding their browser and search engine.

ENDS

78 BEUC testing on HP Windows-operated device on 15 March 2026.



BEUC The European Consumer Organisation

The Consumer Voice in Europe