BCLP. Client Intelligent

Insights

GDPR MEETS DMA: EU GUIDANCE FOR SEAMLESS COMPLIANCE

Nov 03, 2025

As digital platforms dominate our daily lives, a swathe of important EU legislative initiatives has been rolled out by the EU to keep markets fair and data safe. From the Digital Services Act and Digital Markets Act to the AI Act and Data Act, these rules reshape how businesses operate online. At the heart of it all? Data. Personal data powers today's products and services, and new business models thrive on vast datasets and insights. Understanding how these laws interact with GDPR is now essential for anyone navigating Europe's digital economy.

To assist businesses in their compliance efforts, the European Data Protection Board and the European Commission have recently collaborated on draft joint guidance on the interplay between the DMA and the GDPR. Whilst not covering the same ground, and targeting very different objectives, the EU recognises that the compliance with GDPR obligations should be considered holistically with the Digital Markets Act's goal of addressing gatekeepers' data-driven advantages, to facilitate user choice, data access and fair competition.

> "The guidelines will help gatekeepers, business users and individuals to better understand their obligations and rights under the DMA, and ensure a consistent, effective and complementary application of the DMA and EU data protection law." **Anu Talus, EDPB Chair**

We set out below our key takeaways from the draft joint guidance.

SCOPE OF THE DIGITAL MARKETS ACT

The DMA applies to specific undertakings offering core platform services (**CPS**) to users who have been designated by the EU as 'gatekeepers', recognising that these larger platforms will often play a disproportionately significant role in facilitating access to, and use of, the online environment and in doing so, will collect large amounts of personal data from users. To promote fairness, the DMA therefore seeks to regulate how these gatekeeper entities can interact with users, make use of their data and ensure users are free to move between platforms and services, taking their data with them as may be required and enabling interoperability.

HOW DOES GDPR AFFECT BUSINESSES SUBJECT TO THE DMA?

END USER CONSENT

Compliance with Article 5(2) DMA means gatekeepers may not:

- process end user personal data to provide online advertising services;
- combine personal data from one CPS with personal data from any further CPS or from any other services provided by the gatekeeper or with personal data from third-party services;
- cross-use personal data from the relevant CPS in other services provided separately by the gatekeeper, including other CPSs, and vice versa; or
- sign in end users to other services of the gatekeeper in order to obtain personal data.

However, these activities will be permitted if the gatekeeper has given the end user a specific choice to allow their personal data to be used in this manner and the end user has given a GDPR-compliant consent to the use of their data (meaning it has to be freely given, specific and informed). Gatekeepers must also offer a **less personalised but equivalent service** when users refuse consent and cannot repeat a request for consent more than once a year. To ensure a consent is valid from a GDPR perspective, gatekeepers must ensure user-friendly choices (to both give and withdraw consent) and consent designs, notably by streamlining consent requests into a single consent flow, where possible, but ensuring there are separate opt-ins for each purpose. Data controllers also need to ensure it is possible for a user to refuse or withdraw consent without suffering any detriment. Use of pre-ticked consent requests (which are not valid under GDPR) will not therefore be compliant with Article 5(2) DMA. Use of colours and contrasts of buttons, fonts, pictures, or other design choices that may mislead or nudge end users into providing unintended and thus invalid consent under GDPR will risk non-compliance with the DMA.

The gatekeeper is also tasked with ensuring any data processing complies with GDPR principles (including the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy and storage limitation).

APP STORES AND THIRD PARTY APPS

Article 6(4) DMA requires a gatekeeper to enable interoperability of third party apps and app stores with a gatekeeper's operating system and allow these to be capable of being accessed by means other than the relevant CPS of that gatekeeper. It must not prevent any installed apps or app stores from prompting end users to decide whether they want to set that downloaded app or app stores as their default (and must also enable users to change their default choice easily). Whilst recognising that gatekeepers are entitled to take steps to ensure the third party apps do not endanger the integrity of the gatekeeper's hardware/system or affect security controls, these

measures must be necessary and justified and gatekeepers should not seek to instrumentalise their compliance with other applicable laws with a view to make their compliance with Article 6(4) DMA less effective.

The guidance makes clear that gatekeepers (as providers of operating systems) and app developers, should generally be considered as separate controllers under GDPR, and Article 6(4) DMA is not intended to establish any joint controllership or controller-processor relationship between a gatekeeper and an app developer. It emphasises that gatekeepers should pay particular attention to any technical or contractual measures they seek to impose which may be intended to prescribe the way a third party, such as an app developer, complies with the GDPR. As the app developer is a separate and independent controller, it remains responsible and liable for its own processing and should therefore be free to choose how it meets its own GDPR commitments.

Where a gatekeeper may also need to take additional appropriate measures to enable handling of personal data breaches (such as restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident), it must ensure measures taken do not cut across DMA obligations, are appropriate to comply with GDPR and also meet legal requirements stemming from the Cyber Resilience Act.

The guidance also flags the requirement under Article 5(3) of the ePrivacy Directive for end user consent for the storage of information or the gaining of access to information already stored in terminal equipment, unless the processing falls within the exemption (e.g. if these operations are strictly necessary for maintaining the security of the operating system and are user-centric (e.g., setting of a cross-side request forgery token on the user's device)).

The guidance also highlights that gatekeepers should offer access to data, sensors and services on a granular basis to ensure that the beneficiaries of Article 6(4) DMA can selectively access only the parts of the operating system and the data that are necessary for the distribution and functioning of the respective apps or app stores. This is to allow Article 6(4) DMA beneficiaries sufficiently granular control in the gatekeeper's API so that they may limit their access to only that data which they deem necessary for the functioning of their respective app or app store.

RIGHT TO DATA PORTABILITY

A key obligation in the DMA is the requirement to permit effective data portability, on an end user's request and free of charge (Article 6(9) DMA). Article 6(9) DMA complements the data portability right established by Article 20 GDPR (which applies to personal data that has been processed by automated means on the basis of the data subject's consent, or to perform a contract entered into by the data subject). However, the DMA portability right is wider, as it applies irrespective of the lawful ground under which data has been processed by the gatekeeper under the GDPR and requires gatekeepers to enable **continuous and real-time** data portability to end users or third

parties authorised by them. The right covers portability of data that is actively provided by the end user (e.g., identification data provided when signing up for the CPS) and data that is generated through the end user's activity (which includes data created by the end user through their use of the CPS or at the request of the end user of a CPS) and data that is observed by the gatekeeper from the end user's behaviour, such as user engagement with the CPS and data processed automatically or is exclusively processed on device, but excludes **inferred/derived data.**

The guidance flags that since access to on-device data is likely to qualify as access to information stored in the terminal equipment of the end user under Article 5(3) ePrivacy Directive, access to the data by the gatekeeper for the purposes of porting it to the end user or an authorised third party should only take place after the request of the end user (or the relevant third party).

To ensure users can exercise their rights to port their data, gatekeepers must ensure details of their data portability solutions are appropriately visible and accessible, with dedicated and user-friendly data portability online interfaces, supported by comprehensive documentation detailing any rules of access and use, the application process, a data scheme, technical solutions, and timescales.

As authorised third parties are also able to exercise the data portability right, gatekeepers must ensure, from a GDPR perspective, that they have implemented appropriate technical and organisational measures to prevent unauthorised or unlawful disclosure of personal data to unauthorised third parties (i.e. by requesting third parties' identity details and information as whether the relevant data will be transferred outside the EEA, to ensure requests are only processed where the third party is duly authorised to make one).

Gatekeepers must not make data portability conditional upon the use of the ported data and should not seek to obtain details about the third party's GDPR compliance measures — this is not required for the gatekeeper to meet its own GDPR obligations.

BUSINESS USER RIGHT OF ACCESS (ARTICLE 6(10)) DMA

This requires gatekeepers to provide businesses with effective, continuous, free of charge and real-time access to data (including personal data) that is provided or generated in the course of using a CPS. The guidance highlights that end user personal data can only be shared if the end user has given its prior consent, and that this consent is also given in compliance with GDPR rules about consent.

This right of access applies to both aggregated and non-aggregated data, and applies to data directly connected with the use made by end users in respect of the products or services offered by the business user through the CPS.

Gatekeepers must establish user-friendly authentication and authorisation procedures to ensure that only properly authorised business users or third parties can access the data. They must also provide mechanisms enabling business users to obtain end user consent for access to personal data, and ensure that obtaining such consent is not more burdensome than for their own services. Gatekeepers should also inform end users, via privacy policies and dedicated dashboards, about which business users and third parties may access their personal data, and allow end users to withdraw consent at any time (with data access being granular, allowing business users to select specific datasets and timeframes, and should be provided in a format that is immediately and effectively usable).

This right is designed to ensure a level playing field for those businesses who access their customer base via the large platforms that are within the scope of the DMA.

In addition, there is a requirement for gatekeepers who operate online search engines to provide on fair, reasonable and non-discriminatory terms, ranking, query, click and view data to third-party search engines. Any such data that is personal must be effectively anonymised to protect against re-identification while maintaining data utility. Following CJEU rulings on anonymisation and pseudonymisation, the test for determining whether the GDPR standard has been met is whether identification is no longer reasonably likely, considering all means available to the recipient or others, and noting that pseudonymised data can still be personal if re-identification remains reasonably likely.

Gatekeepers who are designated for number-independent interpersonal communications services are subject to an interoperability obligation, for certain basic functions. To ensure compliance with GDPR when an interoperability feature is deployed, it is likely a data protection impact assessment will be required. Gatekeepers must also ensure security parity across interoperable services and process only the personal data which is strictly necessary to facilitate the interoperability. End users must be free to opt in to interoperable features and identity discovery, with consent/choice design developed to avoid 'consent fatigue' and enable simple management across multiple providers. To the extent a gatekeeper implements geographical scope controls, the implementation of these should rely on minimal data, avoid continuous location tracking, and observe the constraints set out in the ePrivacy directive.

Note: We have previously considered how the EU considers online intermediaries / platforms subject to the DSA should approach their GDPR obligations.

If you would like to discuss any of the issues raised in this blog, please get in touch with any of the authors or your usual BCLP contact in London or Brussels (links below).

Geraldine Scali

Dave Anderson

Anna Blest

Marieke Datema

RELATED CAPABILITIES

- Antitrust & Competition
- Data Privacy & Security
- Digital Transformation & Emerging Technology
- General Data Protection Regulation
- Corporate
- Litigation & Dispute Resolution

MEET THE TEAM

Anna Blest

Knowledge & Innovation Counsel, London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475

Geraldine Scali

Partner and EMEA Lead of Data Privacy and Security, London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Marieke Datema

Counsel, London

marieke.datema@bclplaw.com

+44 (0) 20 3400 2132
