www.amcham.ie @americanchamber

AMERICAN CHAMBER of COMMERCE IRELAND

European Commission Consultation on Joint Guidelines on the Interplay Between DMA and GDPR.

Response from the American Chamber of Commerce Ireland (AmCham) to the European Commission.

December 2025

The American Chamber of Commerce Ireland
The Voice of US-Ireland Business

The American Chamber of Commerce Ireland (AmCham) is the collective voice of US companies in Ireland and the leading international business organisation supporting the Transatlantic business relationship. Our members are the Irish operations of all the major US companies in every sector present here, Irish companies with operations in the United States and organisations with close linkages to US-Ireland trade and investment.

Introduction

AmCham Ireland welcomes the opportunity to engage with the European Commission on this important consultation, in conjunction with the EDPB. The DMA and GDPR are critical pieces of legislation that play a pivotal role in the operational efficiency of businesses in Europe, while also providing vital protections for consumers and citizens in the bloc. It is therefore of paramount importance that these pieces of legislation work in a cohesive manner with one another, continue to foster innovation and investment in Europe, ensure the highest standards in safety for end users, and avoid unnecessary complexity.

AmCham Ireland, as a representative body, strongly supports the EU's simplification agenda. By reducing administrative burdens, providing greater clarity of purpose within regulations, and delivering policy that supports end user engagement, Europe can increase competitiveness and attractiveness for investment, innovation and expansion.

The review of the interplay of the DMA and GDPR legislation is a welcome step and represents an opportunity to provide greater clarity and to ensure that companies can operate with certainty, while also providing the greatest level of security and privacy for end users and the wider public.

By addressing concerns within guidelines, including matters relating to data portability, on device data, and the issue of overlapping or inconsistent requirements, the Commission can provide a framework that adequately balances both the DMA and GDPR. In doing so, the Commission can further the protection of consumers and citizens, while also allowing companies to optimise their respective user experiences while meeting obligations set out in legislation.

Portability and Security

It is important that the guidelines particularly regarding data portability, respect the interlinkages of the DMA and GDPR, and in providing for obligations on designated companies, do not undermine the intention of either piece of legislation. GDPR provides for comprehensive data protection and security standards and should remain a core principle of policy development.

The guidelines proposal to establish '*continuous and real time access*' would benefit from further clarity and engagement with stakeholders. The potential of these measures to encompass significant datasets creates difficulties in implementation at a technical level, while also raising potential security concerns as it expands the access and scope of data collection.

This issue is compounded by the inclusion of '*indefinite access*' which, as with continuous access, is a potential cause of major risk and requires adequate data security. This would require designated businesses to provide significant resources to overcome these challenges, reducing time that could be spent on driving other efficiencies within the organisation.

Furthermore, the possible inclusion of other individuals' data as part of a user data request also presents significant challenges with regard to privacy, as well as operational challenges regarding the segregation of data, as well as in obtaining consent. Moreover, requirements that gatekeepers maintain dashboards to track all recipients of third-party data would introduce a significant challenge on an operational level, while also increasing the amount of data being processed for administrative purposes only, creating a further tension with data minimisation goals.

By introducing changes to continuous real time access, and indefinite access, designated companies can ensure that they are providing the best security standards, while also collecting only the data that is necessary, a key aim of data minimisation goals under GDPR and the Data Act. These changes would be strengthened by periodic consent processes relating to data access, the introduction of customisable reminders regarding contest timelines and expiries as defined by the end user, or options to include consent until withdrawn by the user.

Further, with regard to presentation of portability risk notifications, the guidelines outline that this should be achieved in a neutral, objective method that does not infer nudging of the user's behaviour or choice. The guidelines lack clear outlines of what is defined as

nudging in this context. Clarity on this issue must be brought forward as to the role companies can play in line with the requirement to remain neutral but also flag legitimate concerns of privacy and data security. Risk disclosure is an important step in meeting the obligations as set out in GDPR transparency requirements.

On-Device Data

The guidance proposes measures relating to on device data that represent a challenge to both practical implementation and the goal of providing the highest standards in end user safety, privacy and protection.

The development of policies related to mandatory portability for on device data would present significant technical and operational difficulties for businesses in Europe. In some cases, this could also require companies to develop new transfer mechanisms that would operate outside existing secure infrastructure such as cloud services. Underscoring this is the reality that data processed solely on-device, often requires hardware backed encryption keys which cannot be exported in a secure manner. By requiring that this data be portable, the guidelines risk creating new vulnerabilities in security mechanisms.

Moreover, by requiring designated companies to provide measures to capture a large amount of data through on-device data, a further technical challenge for businesses would be presented. Many of these companies do not engage with this on a day-to-day operational basis. The inclusion of on device data further creates scenarios whereby companies are compelled to collect more user data than they need or can use. Inherent to this is an increased security risk, as more user data is stored, increasing exposure in the event of a data breach. Furthermore, this would pose a conflict with stated data minimisation goals, and aspects of the Data Act.

Design Choices

In accordance with GDPR, the DMA requires user consent, this is an important aspect of fulfilling obligations set out in both pieces of legislation and is fundamental to the rights of the individual. The inclusion of obligations on designated companies regarding "*misleading design*", contained within the guidelines, is broad in nature and unclear as to what is defined as misleading or engaging in nudging behaviour.

Greater clarity is needed in order to inform designated businesses as to how these consent options can be presented. This is equally important in terms of clarity and understanding for their users. Accordingly, it is important that the choice required by the DMA, is distinguished from the consent required under

GDPR for processing operation as a combined flow has the potential to introduce additional confusion for end users. By allowing for gatekeepers to exercise flexibility in presenting these choices separately, greater efficiency can be achieved in the operation of the guidelines.

The guidelines include suggestions that colour contrast in relation to consent buttons could be considered as misleading or nudging. However, by removing contrasts on consent buttons, for example, end users could be left without clear understanding as to their meaningful consent, as well as accessibility and visibility concerns that such a decision would raise.

It is in this context that the Commission and the EDPB should not infer, by default, that a designated company is acting in a deliberately misleading manner when offering end users consent options in an effort to provide maximum transparency. By adopting a multi-layered approach to consent mechanisms, which are already viewed positively by some data protection authorities, would allow for greater balance the need for granularity with user experience.

It is important that in this context, that the Commission and EDPB remain cognisant of the potential impact of future consent mechanisms and the need to avoid unduly burdensome consent processes. While many consent processes under the DMA are one-off choices in nature and do not negatively impact on user experience, it is important that future developments do not drive further unnecessary steps that could frustrate designated companies' users or result in 'click-through' behaviours that result in lack of clarity for the user as to what they have consented to.

Gatekeeper - Third Party Engagement

The guidelines relieve designated companies from responsibility in terms of how third parties protect data they receive as a result of a data portability request. While this is intended to clarify, concerns exist regarding the potential tensions with the Data Act, where GDPR takes primacy, as opposed to the DMA guidelines inferring independence from GDPR. This has the potential to create a double standard regarding data portability with different standards being applied under different legislation.

The guidelines would be further strengthened by recognising the privacy and security considerations that derive from DMA Article 6(7). Gatekeepers should retain the possibility to conduct safety and security checks on third parties prior to the transfer of data, where deemed necessary to meet obligations under GDPR.

Furthermore, requirements to keep records on all hypothetical data requests or developing APIs for unrelated third parties would present difficulty when put into operational practice and could further create legal challenges.

With regard to DMA Article 6(10), requirements placed on gatekeepers to facilitate consent interfaces between business users should be carefully considered to avoid unnecessary complexity and user experience issues. It is also important that the DMA does not undermine existing data protection standards, such as data minimisation. Additionally, consideration should be given as to the role of the EDPB and national data protection authorities in assessing gatekeepers' DMA compliance and the impacts on privacy rights as detailed under GDPR. Continued engagement with stakeholders on this matter can aid in ensuring implementation is efficient and achieves the goals of the legislation.

Further, it is important to clarify to extent of a gatekeeper's liability regarding the technical interface provided to business users. This would provide certainty with regard to gatekeeper's liability where subsequent modifications are administered by business users as deemed necessary to their own operations.