

Introduction

The American Chamber of Commerce Ireland (AmCham) is pleased to contribute to the Committee's public consultation on the Pre-legislative Scrutiny of the General Scheme of the Data Bill 2025.

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.

It is vital that the Committee uses this opportunity to develop a forward-looking, practicable, pro-enterprise legislative framework, that also continues to ensure the necessary safeguards for consumers. The Committee should also remain cognisant of forthcoming developments relating to the European Commission's Digital Omnibus Package and the ramifications these interrelated measures will have for Irish society and the Irish business ecosystem.

With many leading technology companies' European headquarters located in Ireland, the 'Country of Origin' principle is of significant importance in ensuring Ireland's position as a key regulatory hub within the EU. Accordingly, the Committee should use this opportunity to develop a coherent, clear, and supportive legislative and regulatory framework that allows companies to invest, grow and innovate in Ireland. By doing so, this will enable the continued enhancement of a dynamic economy, increase Ireland's ability to attract and retain world-leading talent, and support jobs across the country.

The Role of ComReg and the CCPC

The General Scheme of this Bill introduces new responsibilities for both ComReg and the CCPC with regard to enforcement of regulations, as competent authorities. It is important that both authorities are given adequate resources to enable timely engagement with industry, providing compliance guidance for companies, while also establishing mechanisms for industry to engage in meaningful cooperation where an investigation may take place. This is of increased importance given the complex nature of such investigations and requests, in this regard, it is important that companies are given sufficient time to ensure compliance with future regulations. The establishment of a unified user-interface would be of significant benefit to both companies and

authorities, in relation to addressing queries, making submissions and accessing guidance.

Further, greater clarity is required in relation to the introduction of an industry levy to fund ComReg's functions. Such a levy should be clearly defined and proportionate in nature, in order to avoid uncertainty within the business community. Moreover, the Exchequer should provide funding for regulators, along with sufficient oversight with regard to regulator's budgets. Consequently, the inclusion of an industry levy in the General Scheme of the Bill is not comparable with other EU markets and will introduce a competitive disadvantage for the Irish market.

It is important that both competent authorities are also enabled to engage with the European Commission, the European Data Innovation Board (EDIB), other national competent authorities in Member States, as well as industry in Ireland, on an ongoing basis. This is of particular significance given the 'Country of Origin' principle, under which the regulation will operate. As home to many leading technology companies, Ireland occupies a unique space within the EU and therefore should utilise its voice to ensure that regulations are clear, enforceable, and do not result in undue regulatory burdens on businesses.

In line with the competitiveness and innovation goals of both Ireland and the European Commission, it is important that regulatory bodies consider the impact of planned regulations on both competitiveness and innovation in the economy, prior to implementation. Further, by placing competitiveness and innovation at the heart of existing (via review) and future regulations, Ireland and the wider EU can enhance its reputation as a premier destination for investment and growth. In this respect, it is also important that regulators also consider the impacts of new regulations in the context of other existing legislation and regulations and do not act in a siloed manner.

Additionally, it is important that the remit of both ComReg and the CCPC is clearly established to avoid overlapping processes. The Bill should also recognise the role of the Data Protection Commission (DPC), particularly in relation to Head 19, which limits the role of the DPC to matters relating to the use of personal data under GDPR. It is vital that the business community has certainty as to which authority they are to engage with on various matters.

Data Governance

Current European efforts to integrate provisions from the Data Governance Act, the Open Data Directive, and the Free Flow of Non-Personal Data Regulation into the Data Act, resulting in a singular, streamlined framework, is a welcome development that will enhance clarity and certainty, increasing the efficiency of both compliance and enforcement. Despite the encouraging steps detailed above, further clarification will be needed by the business community in order to gain greater efficiencies.

Contained within the Commission's current position is a proposal that has the potential to significantly change the regime relating to cloud switching. Specifically, Article 1(15) of current EU proposals includes a provision into the Data Act setting that a cloud provider may provide for termination charges in contracts of fixed duration other than IaaS (Infrastructure-as-a-Service) contracts.

However, current drafting of wording in the European Commission's Digital Omnibus recognises that *"for reasons relating to financial planning and attracting investment, providers of data processing services, especially SMEs and SMCs, may prefer and offer contracts of a fixed duration. It is necessary to clarify that providers of data processing services may include provisions on proportionate early termination penalties in those contracts as long as they do not constitute an obstacle to switching."*

Despite this, the adopted Data Act definitively reaffirmed that no part of the regulation prevented the parties' contractual freedom of agreeing on proportionate termination charges in line with European Union or national law. This reflects the reality of common practice in B2B engagements and partnerships, where enterprise customers understand that committing to a fixed-term contract is generally more cost-efficient but includes termination charges if ended prior to the commitment end date. These fees are clearly stipulated in the contract and therefore agreed by both clients and providers. In this context, efforts should be made to avoid facilitating the inclusion of an arbitrary exemption to contractual freedom, through the omnibus package.

By introducing distinctions between IaaS, PaaS and SaaS providers, between SMEs and other providers, and including a category of custom-made cloud services (in addition to already existing custom-built services), the regulation creates uncertainty, while also creating the possibility of different cloud switching regimes depending on the type of cloud service and cloud provider. As a result, there is a need to

provide greater certainty with regard to termination fees irrespective of the type of cloud contract.

It is therefore important that a harmonised rulebook is established that reduces the cost of compliance, provides certainty to businesses and encourages the adoption of cloud and related technologies. Integral to this is the need to recognise the differences between IaaS, PaaS and SaaS markets, and the need to avoid a 'one-size-fits-all' approach that would unnecessarily impact on innovation.

Cookies, E-Privacy & GDPR

With regard to cookies and e-Privacy, it is important that efforts are made to deliver effective measures that address the root issues and reduce complexity within frameworks. The ambition to align regulation between GDPR and ePD is an important step in delivering a more coherent policy and regulatory landscape. However, under the European Commission's proposed language, a split remains between GDPR and ePD. Notably, this includes moving regulation relating to personal data on terminal equipment to GDPR, without moving regulations relating to non-personal data, which would remain under the ePD.

This creates a significant problem for the effective and efficient implementation of regulations, as a single cookie often holds both types of data. As a result, businesses would be faced with a complex regulatory landscape, and be required to engage with multiple regulatory authorities for a single file. This can result in increased difficulty regarding enforcement and compliance. The Committee should take steps to ensure that this Bill takes into account the logistical and operational reality for companies engaged in this sector, in line with other laws and regulations.

Further, the Committee should ensure that data access and sharing should be developed in a manner consistent with the principles of GDPR, namely data minimisation, purpose limitation and related legal bases. Additionally, efforts should be taken to ensure that requirements to make data available should be balanced with sufficient safeguards related to trade secrecy, intellectual property, and cybersecurity.

By fully integrating all regulations regarding terminal equipment to GDPR, advancements can be made to enhance the goal of creating a more coherent, simplified process for both enforcement and compliance, while also preventing any compromise of security measures. It is welcome that the European Commission has

acknowledged that the cookie consent system is not working to appropriate standards, serving neither business nor the population.

While there has been a positive expansion to cookie exemptions, the wording of the current language remains narrow and lacks greater ambition. Current frameworks effectively treat low-impact and high-impact operations as the same, being consented to via the same user consent process. This has a net effect of driving consent fatigue, reducing a business' incentive to invest in greater privacy products. The newly proposed exemptions of security and audience measurement are examples of narrowly defined proposals that will lack the ability to significantly alter the current landscape and will also lack the ability to support businesses in developing privacy centric business models, or to reduce the number of consent banners.

Notably, the audience measurement exemption is limited to first-party data. This does not take into account a publisher's frequent reliance on third-party analytics. Nor will the security exemption result in meaningful change to current operations, while areas relating to contextual advertising, such as frequency capping, remain outside of exemptions, even where privacy-centric models are employed, resulting in consent banners remaining in place. Further, by maintaining a narrow scope, there would be no sufficient benefit to B2B organisations utilising data analytics technology, often via third-parties, to facilitate more comprehensive data-driven decision making based on customer insights.