AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

EU Data Act – priorities for trilogues

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.7 trillion in 2022, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

As informal interinstitutional (trilogue) negotiations between the co-legislators are taking place with a view to reach a first reading agreement on the Data Act proposal, the priority for EU decision-makers should be to achieve clarity in the new rules and address the outstanding concerns and ambiguity raised by industry stakeholders across all sectors. In this paper, we highlight our priorities and clarify the following outstanding concerns in the field of cloud switching and interoperability, data sharing, international safeguards and transfers and retroactive applicability.

Introduction

The European Commission's aspirations for a thriving data economy can only be achieved with proper understanding of the impact that the regulatory environment can have across the value chain. Currently, EU policymakers in trilogues are prioritising speed over quality and rushing to reach an agreement on the text which would have significant negative consequences for companies operating in the EU. In this context, AmCham EU would like to give concrete recommendations to the co-legislators as they progress with interinstitutional negotiations in the upcoming months.

Cloud switching and interoperability

Context

Consumers and cloud users increasingly expect measures to facilitate customer switching and data portability. However, any new requirements for providers should be proportionate and feasible – they can't be held responsible for environments they don't control. Requirements should increase, rather than restrict, European user access to diverse, cost-efficient state-of-the-art solutions. The concept of 'functional equivalence' remains problematic as cloud providers can't be responsible for ensuring 'functionally equivalent' experiences in competitor cloud environments with which they are unfamiliar, are not entitled to access, and which they cannot control. The European Commission's proposed approach on interoperability, rather than facilitating switching, also could reduce choice for enterprise customers in Europe, lead to less innovative features on offer and potentially conflict with international IP (TRIPs) commitments. Proposed changes to contracts and prohibitions on reimbursement of any switching costs would significantly impact current cloud contracts and fixed-term and long-term deals, which would result in higher prices for all customers rather than enhanced switching.

Recommendations

Functional equivalence

We support that Chapter 6's 'functional equivalence' requirements remain limited to IaaS with the explicit exclusion of PaaS and SaaS delivery models (recitals 72 in the European Parliament and Council texts) and encourage alignment with corresponding requirements in the interoperability chapter. Also, and while the concept remains problematic, the Parliament's revised definition of functional equivalence in article 22a and recital 72, and the Parliament's clarifications in article 26(1) represent improvements (while the concept remains unworkable in other versions) These revised articles clearly call on the destination provider to play its part in allowing for functional equivalence requirements to

work, as the source provider cannot make it work on its own. Modern ICT applications are built on a rich and constantly evolving set of resources that offer choice in terms of capability, performance, cost, and other factors. Customers choose their data processing service often based on several factors, including the special features offered. Requiring all cloud service providers to use the same specific technologies or data formats would result in uniformity of software services leading to reduced choices for customers and discourage the development of more innovative offerings in the EU.

Flexibility

Additional flexibility is needed in proposed contractual requirements. We support the clarification made by the Council that fixed-term contracts remain lawful (recital 72b) and would recommend its adoption in the final text. We also welcome the longer notice and transition periods put forward by the Parliament (articles 23 & 24). However, we would recommend the introduction of contractually agreed alternative periods between the cloud provider and the customer in the notice, termination, and transition contexts. This approach would better ensure freedom of contracts and provide the ability of EU businesses to negotiate price reductions in exchange for fixed-term (multi-year) contracts.

Switching requirements

The scope of the switching requirements should be clarified. In particular:

1. Support the Parliament's exemption for custom-built services in article 26a(1) which allows for a flexible cloud services market and encourages cloud uptake. Services which are custom-built to meet specific client needs cannot be subject to the switching requirements since these are far from being utility-like services.
2. The concept of 'equivalent services' should be clear and applied consistently throughout the Chapter. Currently, this concept is used in articles 23 and 26, and in the definition of switching in article 22a(6), but not in article 24. This creates a major and problematic loophole. How can the obligations under article 24 apply to all data processing services, even when not equivalent? Lastly, an amendment to the definition of 'equivalent services' should be considered because its criterion (sharing the same 'data processing service model') is unclear (what is a 'data processing service model?'). We would, accordingly, suggest the following definition: 'equivalent service' means a set of data processing services that share the same primary objective and data processing service delivery model and can achieve syntactic and semantic interoperability.

Switching process

The importance of the technical description of the switching process should be acknowledge by allocating responsibilities to the right actor. Transition (switching) processes are often complex and fragile exercises – if they fail, they can lead to failure of critical infrastructure. Therefore, the technical description of the switching process should be tailored to technical reality of the transition projects, which should not be artificially modified through regulation. Moreover, not all data should be shared between competitors, or is necessary for clients to receive services from the destination provider. This should be acknowledged by preserving the Parliament's definition of 'exportable data'.

Existing contractual arrangements

Policymakers should take into account existing contractual arrangements between cloud providers and cloud customers, as well as the specific legal and financial obligations of those cloud providers that are publicly traded companies. Specifically, we have concerns regarding the appropriateness of the proposed contract minimums for B2B data processing services, as such contracts are negotiated between sophisticated parties and often operate on multi-year terms.

Good faith obligation

Support the adoption of the 'good faith obligation' article (24b) introduced by the Parliament for all parties involved in the switching process. Switching is not a one-step process and not solely under the control of the exporting data processing service provider. Effective, secure and timely switching requires not only co-operation but also, and most importantly, expertise at both the exporting and the importing data processing provider level.

Portability and interoperability

There should be alignment with international standards bodies and a limited involvement by the Commission in the portability and interoperability chapters. Standards should be developed through consensus-based, market-driven, fair, inclusive and transparent processes that leverage or build on existing standards from the International Organization for Standardization (ISO)/the International Electrotechnical Commission (IEC) and other leading international standards bodies. In that sense, we support the clarifications made by the Council in article 29 to limit the role of the Commission in the adoption of common specifications, and to not limit specifications to European standards only. A standards-driven approach to interoperability and portability should be based on globally focused, multi-stakeholder standards settings organisations with governance models that are open, inclusive, fair and balanced to guarantee a diversity of perspectives and solutions. This in effect would be the best way to promote the European perspectives and values. The Data Act should avoid imposing rigid standards for portability, while taking specific situations and contexts into account and considering the data at play, their volume, the operator concerned, and available alternatives.

Data sharing (IoT, B2B, B2C)

Context

While we welcome the Commission's objectives to foster data sharing and re-use, we are concerned about implications for trade secrets resulting from mandatory data sharing obligations. EU requirements should not introduce obligations to share trade secrets, as their protection is essential for the competitiveness of all businesses in Europe. Companies should not be required to share data – their own or that of their customers – which is confidential or would constitute trade secrets without adequate protection and/or data holder's consent. Also, we would welcome greater clarity to the scope of products covered. Currently, the Parliament and the Council texts move from having an IoT focus to potentially pulling in scope all kinds of products on the basis that they can connect to the Internet (recital 15), introducing new and unclear obligations and impacts on more complex environments without adequate impact assessments.

Recommendations

Mechanisms to protect trade secrets

We welcome the introduction by both institutions of further mechanisms to protect companies' trade secrets and would recommend their adoption during the negotiations. The Commission's proposal, rather than clarifying, creates ambiguity regarding a potential weakening of existing protections for trade secrets. The introduction of additional safeguards (articles 4[3] and [8] in the Parliament's text and article 4 [3a] in the Council's version), with the possibility for the data holder to refuse the request for data access under exceptional circumstances is a positive step to reinforce companies IP and trade secrets protections. However, businesses should not have to demonstrate potential bankruptcy or a threat to their viability to be entitled to refuse to share trade secrets. The threat of a serious damage should suffice.

Definitions of in-scope data

Reconcile definitions of in-scope data, including 'inferred data' and 'exportable data' to provide clarity and protect trade secrets. Data which is derived or inferred is exempt from the scope of the Act (recitals 16, 23a, 24b; articles [3], 4[1]) Yet, the new definition of exportable data in article 22a includes 'output data' within scope for switching obligations. While the carve-out for IP and trade secrets is helpful, the inclusion of output data in this definition confuses the boundaries between what data are in and out-of-scope for the Act. The draft also expands the Act's scope to inferred data relating to physical quantity/quality changes (recital 24b). The introduction of this provision could have significant impacts on industrial data holders, singling their products out and exposing their IP to additional risk without a clear policy purpose. The definition of exportable data should not include output data or derived/inferred data, consistent with the scope of the Act. In addition, clarification on what constitutes 'inferred' or 'derived' data would promote regulatory certainty.

Definition of data holder

We support the Parliament's clarification of the 'data holder' definition laid out in article 2(6) with the mention of the 'contractually agreed right to use such data' and would recommend adopting this definition in the final text. This would ensure that entities, such as data processing services/software providers, who are generally contractually prohibited from producing customer data without their consent, would not be forced to do so with this new data access right.

Definition of related service

We would welcome clarification of the definition of 'related service' in article 2(3) because it continues to be overly broad. This is particularly concerning given the expansion of the definition of 'product', mentioned above. Related services should be in scope if they are necessary for the product to perform one of its essential functions, which no other service could similarly facilitate. Otherwise, virtually all services that could theoretically be used with a product to perform even ancillary functions would be captured. We welcome the clarification in the Council text that services must be interconnected with the product 'at the time of the purchase, rent or lease agreement' to qualify as related services to begin with. However, we ask that the text further clarify that the service is necessary for the product to perform an essential function.

International safeguards and transfers

Context

Potential prohibitions on international transfers of non-personal data could limit European companies' ability to leverage available state-of-the-art technologies which cannot be offered in

localised environments. Questions about the consistency of the proposed prohibitions with free trade obligations and EU commitments (eg Regulation on the Free Flow of Data, the World Trade Organization [WTO] commitments, etc) remain. Non-personal data is far less likely to be subject to government access requests and does not raise the same level of risks as personal data. Also, the Data Act provisions on international data transfers will require the IT sector to monitor clients' data at all times, and then decide if data should be transferred, and what measures to apply to safeguard data when transferred - whereas clients should remain in control of their data. Article 27 will therefore lead the exact opposite outcome than its stated objective – give users control over their data.

Recommendation

Requirements in article 27

We recommend clarifying ambiguous article 27 requirements so that it cannot lead to diverging interpretations resulting in localisation requirements. The Data Act should contribute to enabling, rather than restricting, the free flow of data, and should facilitate cross-border data sharing to leverage its collaborative benefits. Data localisation requirements, intentional or unintentional, could also hurt sectors that do not participate heavily in international trade such as healthcare, where up to a quarter of inputs, for example, consist of data-reliant products and services. We recommend clarifying that, where a provider's systems store personal data, any existing adequacy findings, Standard Contractual Clauses (SCCs) and corresponding Transfer Impact Assessments (TIAs) under General Data Protection Regulation (GDPR) should be sufficient without duplication of obligations under the Data Act.

Alignment with international rules

Policy makers should ensure alignment with EU international rules and commitments. Current provisions could create impediments to companies' ability to transfer non-personal data like those that the GDPR imposes on personal data. Such restrictions may be inconsistent with the EU's commitments under the WTO's General Agreement on Trade in Services (GATS), under which the EU has committed not to restrict cross-border provision of data processing.

Personal and non-personal data

We recommend addressing the potential for great complexity when international data transfers contain both personal and non-personal data. Having two separate standard contractual clauses with different requirements regulating the transfers of both personal data under GDPR and non-personal data under the Data Act may create friction and legal complexity when dealing with data transfers.

Retroactive applicability

Context

The report from the Parliament states that data holders' obligations towards users article 4(1) will apply to related services placed on the market 'within five years prior to the entry into force of this Regulation'. Such retroactive applicability of a new EU regulation would create a severe business impacts and compliance burdens, if not impossibilities.

Recommendation

Recommend retroactive data access proposal to be removed from the obligations resulting from article 4(1), as certain products and related services have not been designed to accommodate such requirements. Additional problems would include, for example, a machinery manufacturer pays for the telematics and telecommunications subscription for its products, which is provided by a supplier. Customers can always get the telematics service and access to the related data, but are required to pay a fee – ie customers have the choice to take this option or not. If with the retroactive applicability in the Data Act the manufacturer would need to give customers access to the data for free, it will create an unfairness for the customers that have historically paid for the telematics service during those five years prior to the implementation of the Data Act.

Conclusion

AmCham EU supports the overall objective of the Data Act Regulation to increase data access and use. As the policymaking process accelerates on this crucial proposal, industry warns against possible unintended economic consequences across data value chains. It is in the interest of both industry and EU policymakers to find a workable solution for the above mentioned concerns in order to build a framework that supports Europe's data economy.