AmCham Estonia
American Chamber of Commerce Estonia

DIGITAL RESILIENCE

AmCham Estonia
American Chamber of Commerce Estonia

DIGITAL RESILIENCE

AMCHAM ESTONIA DIGITAL SOCIETY COMMITTEE POSITION PAPER

INTRO

Digital technologies have the potential to solve some of society's most difficult challenges, such as climate change and healthcare, and foster the birth, development and growth of new ventures that will create and finance the future of Estonia.

As a Digital Frontrunner, Estonia has a good chance to reap the benefits of digitization, however it requires that Estonia continues to drive an ambitious national agenda on digitization, innovation and entrepreneurship. But since Estonia is a small and export driven country, it's success largely also depends on the EU's ability to develop a positive policy agenda that promotes open economy, free trade, digital innovation and transatlantic relations and that avoids protectionism and harmful regulation. On that note, we strongly support the recent letter that Prime Minister Kaja Kallas and nine other Prime Ministers sent to Ursula Von der Leyen, highlighting key elements such as the need to focus on long-term competitiveness, "open strategic autonomy", new innovative technologies, better regulation, data flows, an ambitious trade policy and cooperation with key partners. We urge Estonia to continue to use its role as a digital leader and soft power to push for a positive agenda, including by working closely with partners and like-minded countries.

1. Geopolitical crisis calling for policies that are secure by design

It's more than a year since Russia's unprovoked invasion of Ukraine and the war continues to be a tragedy. We stand firmly with the people of Ukraine as they face incredible suffering and we will continue to do so. Russia's actions are threatening the fundamental values upon which our societies are based and we are cognizant of the importance of this war, both for the people of Ukraine, for broader geopolitical dynamics and cybersecurity. Given the current crisis, it is clearer than ever that policies need to be secure by design and that we should further the cohesion of the Transatlantic alliance. Also, we support the idea to create a dedicated mechanism at EU level to ensure that all technology policy initiatives and regulations are assessed for unintended effects on security and alliance cohesion as proposed by the Munich Security Conference.

2. Estonian Digital Agenda and Broadband plan for 2030

To use the full potential of digital era and to fulfil Estonia's Digital Agenda and Broadband Plan there is need to **simplify the construction of electronical communication networks incl 5G masts in Estonia.** Among other things, it means that electronical communication infrastructure should be normal and legally required part of all construction projects (construction of roads and buildings). This also supports the construction of innovative mobility solutions e.g. "smart roads" and reduces CO2 emissions, i.e. thus supports meeting the climate goals.

We also see that to accomplish the digitalisation agenda and the best connectivity experience everywhere in Estonia the **state aid funding** for building very high-speed broadband networks in rural areas (so called white/market failure areas) needs to be remarkably increased by the state. Currently, majority of investments to broadband networks comes only from certain private sector operators. To meet EU connectivity targets everywhere (also in more remote areas of Estonia), more extensive state aid funding is necessary by government to ensure very high-speed internet connectivity in all regions.

3. International transfers of personal data

We are in a moment of economic crisis and without a new data transfer agreement between the US and the EU the economy could be further disrupted. It is imperative that data flows continue from the EU to the U.S. to support the $7.1 trillion in transatlantic trade and investment. Data transfers are the bedrock of the transatlantic relationship and are essential in keeping the businesses, citizens and communities connected. There is a significant risk of real-world harm if data flows are disrupted or interrupted.

Following the publication of the draft implementing act by the European Commission on the EU-:US Data Privacy Framework, the European trade associations DigitalEurope and BusinessEurope joined efforts to commission an independent legal analysis to assess the European Commission's draft adequacy decision on the EU:US Data Privacy Framework. Amongst the findings of the study, it concludes that considerable efforts have been made by the US to improve the current framework if compared to the previous one, specially related to necessity, proportionality and redress. It also states that these efforts can meet the legal test established by the EU Court of Justice.

We encourage the Estonian government to actively push for a successful adoption of the agreement as otherwise the data transfer hindrance between US and Europe will be not solved in practice.

4. DMA: Should apply to all clear gatekeeper candidates regardless of origin.

The DMA should remain true to its ambition to level the playing field in digital markets among all clear gatekeeper candidates, regardless of their country of origin. This will require issuing timely designation decisions for all companies meeting the thresholds of the DMA.

We understand that the DMA has been designed to capture at least a handful of American tech companies primarily. However, it increasingly becomes clear that popular companies from other regions of the world, like TikTok, are very likely to meet the quantitative thresholds. Accordingly, the Commission should strive to designate these companies as soon as possible.

We consider it important that the DMA does not grant an artificial competitive advantage to companies from other regions of the world amidst increased geo-political tensions. In the same vein, the DMA should not work to disadvantage US companies only. It could strain the EU-US relationship if all designated gatekeeper companies end up being American while obvious gatekeeper candidates from other regions of the world are left out.

5. AI

We believe in the positive contribution AI makes, but we also recognise that the use of AI raises certain concerns. AI is not itself inherently good or bad; the key is developing and deploying it responsibly and ensuring regulation is risk-based and use case specific while allowing for continued innovation and practical implication of this transformative technology. The EU is currently discussing how to regulate AI. We support the Commission's objective to ensure a proportionate, risk-based approach to AI regulation, and hope this can be a helpful start for a global discussion around AI governance.

However, we are concerned that some proposed amendments from the European Parliament and the Council dramatically expand the scope of the original proposal for the AI Act in ways that could raise the cost and limit the availability of low-risk AI in the EU, undermining innovation and competitiveness in Europe, limiting interoperability of markets while providing few benefits to consumers. We urge Estonia to advocate for a risk-based and use case specific approach and ask for a regulation that only focuses on applications that will potentially cause significant, irreversible harm and not on the technology itself. The AI Act should leave room for innovation in AI and general-purpose AI (GPAI) technologies as they are used by many developers, startups and SMEs in Europe.

Concrete recommendations:

- The list of high risk AI applications should not be over-broad in scope. The list should reflect only genuinely high risk usage. There is nothing inherently risky about the AI technology powering recommender systems for user-generated content. A recommender system should not be treated as high-risk on the mere basis that it is

a recommender system. Furthermore, regulatory frameworks already exist - i.e. GDPR and DSA - regulating the way personalisation and recommender systems work. In particular, recommender systems are already subject to a wide range of requirements under the DSA. The DSA should be given time to apply before additional requirements are introduced.

- Significant technical documentation and assessment requirements would lead to a slow down in deployment of recommender systems that would have detrimental consequences, including:
    - Depriving consumers and businesses of all sizes of the many benefits of these systems, including the ability of small businesses to reach customers and grow their businesses and the ability of consumers to learn more about timely events in their local community.
    - Making it harder for platforms to ensure an age-appropriate experience, or to deliver content in the correct language, or location.
    - Making it harder for platforms to keep bad actors and malicious activity off of their platforms.
- Purpose-agnostic technologies like GPAI/foundation models should not be classed as high-risk en-masse, but evaluated instead based on the risk of the applications in which they are embedded.
- Generative AI (GA) does not need to be singled out for special treatment. It should be covered by the rules for GPAI, and transparency provisions within Article 52.
- When it comes to GA it has also been proposed that providers should disclose training data protected under copyright law. But most models are trained on web crawled data and it is practically meaningless to summarize the entire open web. The proposal is neither necessary nor justified. The European Commission recently clarified that copyright holders are already protected with regards to this content by Art 4 in the EU's Copyright Directive which allows right holders such as publishers to opt-out of text and data mining.
- Non-commercial and open-source general purpose AI/foundation models should be exempt, so as to promote research and innovation, and encourage broader access to large scale AI models.
- The terminology of the Act (e.g., "provider" and "user") does not sufficiently distinguish between roles in the AI value chain (i.e., AI developers, deployers, end users, and other actors); and the Act's obligations do not consider these parties' different roles or provide clarity on which parties are responsible. Companies want to understand clearly how and when to comply with the requirements of the Act. Clarification is needed on which parties have responsibility for the obligations under the Act. It should be made explicit that deployers who use GPAI in high-risk applications are best placed to understand and effectively manage risk, and meet legal requirements.
- Providers and deployers should maintain contractual freedom to ensure risk is suitably covered without creating unnecessary risk. As is common in manufacturing and in the GDPR, deployers can require that developers make contractual commitments to assist them with compliance.
- Lastly, we seek commitment from the EU that it will align the AI Act with international standards and definitions, e.g., as developed in the OECD, to ensure interoperability of AI services and regulatory regimes and respect for existing bilateral regulatory engagements.

6. Product Liability Directive

The EU Commission's proposal for a revised Product Liability Directive (PLD) proposes extending strict product liability rules to software and related services. We support the underlying objective to ensure a high level of legal certainty for companies and trust for consumers, but we strongly caution against the inclusion of stand-alone software in the PLD because strict liability deviates from the legal norm that liability should entail fault and is reserved for situations that bear a risk of severe damage to persons or property. Also, strict liability for standalone software will in most cases not be justified given software's fundamentally different nature and risk profile from physical goods. Soft-

ware can be readily fixed through remote updates, and bugs are generally accepted as inherent to software development. Software developers often lack control over how their software is integrated along the supply chain, and standalone software cannot physically act upon any person or property. This greater legal exposure for software developers could have profound unintended consequences, such as: i) a chilling effect on innovation and digitization in Europe; ii) higher priced devices and software, to compensate the manufacturer/developer for higher potential costs; iii) worsened software performance and a trend toward basic functionality for users (in light of the security-performance trade-off for software development); iv) potentially holding developers liable for user harm caused by taking action to prevent exploits (for example, where taking such action results in lost user data); (v) reduction in coverage of, or complete removal of, useful factual information made available by the software.

We also believe the extension of damages to material damages caused by psychological harm will lead to great legal uncertainty. As written, the provision does not propose sufficient conditions that must be met to link psychological harm with any single product. Unlike physical injury, psychological harm depends greatly on the consumer at hand and their given context. Requiring that the psychological harm be "medically attested" is an insufficient threshold. Ideally, several psychiatrists or physicians would need to be consulted and ideally, these professionals would be court-appointed for absolute objectivity. Including it as a damage in a no-fault liability regime introduces great legal uncertainty and a constant risk of litigation, as economic operators will find it impossible to predict where one consumer may experience psychological harm whereas many others will not.

Though the Commission's proposal does not reverse the burden of proof, the text presents a de facto reversal for scientifically or technically "complex" products (Article 9.4). This notion is undefined in the text (though Recital 34 provides several examples and names outright e.g. machine learning) and open to the discretion of national courts, making it unclear to economic operators whether their product will be determined complex. These Articles (as well as Recitals 3 and 34) put digital products and services, advanced software, AI systems on unequal footing vis–à-vis more traditional moveables.

The disclosure of evidence also presents a problem in that it is very broad and the provisions for confidentiality (Article 8.2-4) are too weak. It is imperative that confidentiality safeguards apply to all disclosures and not only information "used or referred to in the course of the legal proceedings" (Article 8.4). The PLD proposal also fails to detail the consequences in the event that there is a confidentiality breach. We also note defendants do not enjoy similar rights to request disclosure of documentation (such as proof of purchase, regular data back-ups, or heeding of company warnings about product use) to prepare their defence, as should be the case. This balance is important, especially given that a defendant's refusal to disclose evidence invokes a presumption of defectiveness (Article 9.2.a).

We are also concerned about the extension to cover 'related' services, that there is no precise definition of software, new disclosure mechanisms and that it introduces no-fault (strict) liability for online marketplaces which goes further than the Digital Services Act. We hope that Estonia can play a positive role in improving the proposal.

7. European Media Freedom Act

We support the Commission's objective to safeguard media pluralism and editorial independence, but we are worried about article 17 which suggests implementing a mechanism whereby the identification of media service providers (MSP) is based on self-declaration, without any third-party verification or safeguards. As the proposal is written, almost anyone can claim that they are an MSP without any checks and balances. Given how the criteria are set out in the Regulation, Russia Today would have qualified as a media service provider deserving of these additional protections if the law had been in place just a few years ago. It's hard to believe that Russia Today wouldn't have been protected and that would have made it difficult for platforms to take quick action when Russia started to invade Ukraine and escalated its disinformation activities.

We have also seen rogue actors impersonate media services in the past to post harmful content. As it stands, there are no safeguards to prevent this type of abuse. In addition, by expecting Very Large Online Platforms (VLOPs) to decide whether to accept a self-declaration, article 17 and Recital 33

are placing the responsibility of determining who qualifies as a media service provider on VLOPs – yet VLOPs are not equipped to apply the criteria currently outlined in article 17 across 27 different Member States. We are worried that it will become much harder for platforms to fight against e.g. harmful disinformation if bad actors will be granted a special privilege so that platforms cannot stop their harmful content from spreading. As the war in Ukraine has shown, it is important that platforms are ready and agile to respond to new and emerging threats. The EMFA must not be a step back in the fight against misinformation/disinformation and it must be compatible with and acknowledge the frameworks already in place in existing EU laws, notably the Digital Services Act, the EU Code of Practice on Disinformation, Audiovisual Media Services Directive, the Digital Markets Act - all which have been recently adopted or implemented. It's important to remember that actions taken by platforms under their community guidelines or terms of services are not left unchecked. The Digital Services Act requires providers of online platforms to provide internal complaint-handling systems (Article 20) and out-of-court dispute settlement (Article 21) for those who disagree with them (including MSPs). So there are already sufficient safeguards for MSPs when VLOPs moderate their content. We urge Estonia to push for improvements that ensure full harmonization with the DSA.

Ultimately, legislators need to improve the text by:

- Narrowing the definition of media service providers in Article 2.
- Introducing some form of verification of an MSP declaration e.g by regulators, civil society or third parties.
- Introducing a vetting mechanism for a list of bodies that are certified as co- or self-regulatory bodies.
- Introducing some form of penalties for misuse. This could be along the lines of what was agreed under the DSA, whereby Trusted Flagger status can be revoked if it is abused.

8. DATA ACT

The Data Act will introduce requirements on cloud portability and data sharing. The Data Act aims to "ensure fairness in the allocation of economic value among actors of the data economy". While we support the objective of the proposal, we are concerned that certain obligations such as mandatory B2G data sharing or to share data that contains trade secrets or is protected by intellectual property rights might have unintended consequences for the IoT industry. Also, the alignment between the Data Act and GDPR still raises problems and might have serious concerns around users' privacy and security.

We are concerned to see that the Parliament and the Council expanded the scope of the definition of "product" in a disproportionate manner compared to the objectives of the Data Act. The texts moved from focusing on IoT and industrial devices to essentially pulling in scope all kinds of products on the basis that they can connect to the Internet. This is disproportionate to the objective of the Data Act. The Data Act should not apply to products which are primarily designed to create, display, play, record or transmit content; and not prone to produce data that is relevant in an industrial or IoT context; regardless of whether those products may also be able to obtain, generate or collect some IoT data concerning their use or environment.

We are also concerned to see that Article 5(2) of the proposal – which prohibits undertakings designated as gatekeepers under the Digital Markets Act (DMA) from being data recipients – has not been properly addressed. If the main objective of this proposal is to increase user choice and competitiveness, excluding certain companies from the outset limits the potential consumer benefit and reduces the incentive for those companies to build tools to facilitate portability. Further, the restriction for DMA gatekeepers is overly broad as it will prevent gatekeepers from obtaining data for the provision of services that might not reach the thresholds to be designated as "core platform services" under the DMA. While we continue to believe the restriction for DMA gatekeepers must be removed completely from the Data Act, we expect it would be at least aligned to the DMA and be exclusively scoped around the services offered by gatekeepers which will be designated as core platform services under the DMA. The EU agency BEREC was also critical of this prohibition in its opinion on the Data Act.

While we support the Commission's goal to enhance the multi-cloud industry in Europe, we think that certain provisions such as the definition of "functional equivalence" and switching deadlines should be clarified in the cloud switching chapter. The prohibition on charging fees for switching cost, (and even data transfer for multi-cloud use in the Council proposal) is disproportionate. We welcome the Parliament's position on cloud switching and hope that the policymakers will be able to find a workable solution in trilogues. Finally, on international non-personal data transfers (Article 27) **we welcome the clarification made by the Council that Article 27 relates to international governmental access and transfers of non-personal data.** However, there is still a substantial amount of legal uncertainty in Article 27 that has to be yet addressed. Especially, how it aligns with GDPR and the transfers regime on personal data. Where a cloud provider's systems store personal data, any existing adequacy findings, Standard Contractual Clauses (SCCs) and corresponding Transfer Impact Assessments (TIAs) under GDPR should be sufficient without duplication of obligations under the Data Act.

We encourage Estonia to closely follow these key issues during the trialogue negotiations on the Data Act.

9. EU Cloud Security Services

The EU Cloud Services Certification for Cybersecurity ("EUCS") has the potential to drive a step-change in baseline European enterprise and public sector cybersecurity for cloud deployments particularly in light of the increased risks posed to European security in 2022. However, the inclusion within the scheme of provisions related to data and operational sovereignty would fundamentally depart from established international cybersecurity standards and present a serious barrier to widespread adoption. Security operational best practice and resilience will suffer as cloud customers will lose their ability to implement global security mitigations, benefit from threat telemetry data gathered from other regions and move data from compromised regions to secure storage centers as attacks unfold.

It best serves European cybersecurity interests to progress with a narrowly focused, technical scheme (ie. removal of the sovereignty controls) rapidly. Political dialogue about digital sovereignty should be separated from the EUCS debate and ultimately resolved in a way that allows national states to determine whether specific controls are necessary - and whether the trade-offs those controls may pose for security and cloud-led innovation are acceptable to meet their national digital sovereignty needs.

10. International tax reform

The OECD is negotiating a global tax reform with the aim to reallocate taxing rights targeted at the world's largest companies (Pillar 1) and new standards around global minimum taxation (Pillar 2). We are supportive of the OECD process, and we are hopeful that Estonia will continue to support a robust, multilateral framework that doesn't discriminate against products and services, and we hope that harmful targeted taxes such as Digital Services Taxes (DSTs) will no longer be considered at national or European levels. DSTs are problematic in that they narrowly target certain activities and companies and are designed to operate outside the principled framework of business taxation. They create concerns around tax and legal certainty and the legitimacy of an international tax system that has been built around multilateral coordination. This is the system that underpins all global trade and cross-border investment and the reason why it's important that Estonia supports the OECD framework.

AMCHAM DIGITAL SOCIETY COMMITTEE (DSC)

Purpose of the Committee:

DSC is investigating how digitalization has an effect on individual preferences, social values, corporate goals and public policy-making. Our aim is to raise awareness among companies and Estonian public in general by introducing best practices in managing and benefitting from technological innovation. We do so by arranging thematic workshops and speaker events with local and foreign professionals.

DSC focuses on the following topics:

- R&D and Intellectual Property
- Digital Single Market
- 5G
- Data protection and international transfers
- AI
- E-Commerce
- Cyber Security and Online Safety