

DIGITAL COMPETITIVENESS AND THE TRANSATLANTIC EDGE

KEY EUROPEAN DIGITAL FILES, 2026 TO 2027

AMCHAM ESTONIA DIGITAL SOCIETY COMMITTEE POSITION PAPER 2026

WHY THIS MATTERS NOW

As Estonia prepares for its parliamentary elections, Europe is still deciding where the next wave of digital and AI investment goes. Europe has most of what it needs to succeed in the AI era: a large market, strong positions in the chipmaking supply chain, stable institutions and strong technical talent. What it lacks is the one input policymakers control directly, namely the rules that let it build. On its current path, Europe's own rules will not let it invent, lead and thrive, and investment, talent and vital AI capabilities will keep migrating elsewhere.

Estonia has more at stake in that than most Member States, and our members are part of the answer. AmCham Estonia's members include major international technology companies that are significant investors, employers and innovation partners in Estonia and across Europe. Estonia's digital success has been built on openness, innovation, and access to best-in-class technologies, and on a close relationship with the United States. Estonia's own experience during geopolitical crises has shown that globally distributed cloud infrastructure preserved government continuity precisely when local infrastructure was at risk.

The numbers show how far the gap has opened. Europe holds only around 5 percent of global AI compute against 75 percent in the United States and 15 percent in China, and is a net importer of AI compute. It attracts around 6 percent of global AI venture capital against 75 percent for the United States. Money follows predictable, innovation-friendly rules, and Brussels and national capitals legislated their way into these numbers.

Four files will decide whether that changes in this parliamentary term. They sit in different Council formations and different parliamentary committees and are almost never discussed together, but each one asks the same question: can a company working from Estonia get the technology, the data and the legal certainty it needs to compete. We ask the current as well as the next government and Estonia's MEPs to treat them as priority.

1. CLOUD AND AI DEVELOPMENT ACT (CADA)

The [Cloud and AI Development Act](#) is part of the Commission's Tech Sovereignty Package. AmCham Estonia supports the objectives of strengthening Europe's digital resilience, cybersecurity, technological capacity and AI competitiveness. These goals matter for Estonia and for Europe's long-term security and economic growth. We welcome the ambition to expand EU data centre capacity, foster sustainable computing, and ensure operational continuity of cloud services for the public sector.

Our concern is that the proposal as drafted equates sovereignty with corporate nationality instead of with verifiable technical and operational controls. That risks limiting European customers' freedom to choose the solutions they need to stay secure, competitive and innovative. What should matter is whether an organisation can keep control of its data, keep critical systems running under pressure, move workloads, and combine services across providers. Only technical design, breadth of services, dedicated partnerships, and independently audited controls and assurances can demonstrate that. Corporate nationality cannot.

For Estonia this is a critical issue. If trusted non-EU providers are restricted from serving the public sector, critical infrastructure or other important customers, Estonia may face fewer choices, higher costs, slower innovation, and weaker access to advanced cloud, AI and cybersecurity capabilities. That is the paradox at the heart of the regulation: the most critical public sector workloads are precisely those most urgently in need of frontier AI capabilities, advanced cybersecurity tools and global-scale threat intelligence.

Three provisions do most of the damage. The Union Assurance Level framework grows progressively more restrictive, culminating at UAL 4 in a requirement for a fully EU-controlled software supply chain that no cloud provider, including European ones, can currently meet. The third-country regime in Article 18 would not automatically extend eligibility to the United States, Canada or the United Kingdom; unlike the Chips Act, which extends eligibility to GPA and FTA partners, CADA excludes foreign providers by default, with no timeline or obligation on the Commission to decide on exceptions. And Article 29 delegates the risk assessment methodology entirely to a post-adoption implementing act while the Commission keeps power to override Member State assessments, which removes the ability of contracting authorities to determine how best to mitigate risk and recognises neither multi-cloud strategies, contractual exit plans nor customer-managed encryption as legitimate alternatives.

WHAT WE ASK ESTONIA TO DO

- Support an approach based on open sovereignty: strengthening European capabilities while preserving cooperation with trusted global partners. The proportionate response to operational continuity concerns in adverse political scenarios is resilience, not exclusion.
- Insist that strong technical measures, including customer-managed keys, split-key schemes, zero-knowledge encryption and confidential computing, count towards higher UAL eligibility irrespective of corporate nationality.
- Remove UAL 4 entirely, recognising that defence-specific requirements should remain outside the scope of CADA.
- Reorient the instrument from origin-based restrictions towards outcome-based requirements: define what a provider must demonstrably deliver, meaning verifiable data control, operational continuity, jurisdictional safeguards and transparency, rather than prescribing who a provider must be.
- Include GPA and FTA partners in UAL 3 by default, consistent with the Industrial Accelerator Act and the Chips Act, to preserve legal certainty and avoid triggering reciprocal trade restrictions against European companies abroad.
- Remove or substantially limit the Commission's power to override Member State sovereignty risk assessments, preserving national discretion based on local security and digital needs, and subject the Article 29 methodology to co-legislative scrutiny with a rigorous impact assessment covering costs to national budgets, effects on innovation, and consistency with the EU's commitments under the WTO GPA and bilateral trade agreements.
- Remove the Article 31(3) mechanism for extending sovereignty requirements to the private sector without full co-legislative procedure and mandatory public consultation, which as drafted creates systemic legal uncertainty across the NIS2 Annex I sectors.

We recommend that the Estonian Government take note, in the context of CADA, of the ongoing debate over the Industrial Accelerator Act's 'Made in Europe' and 'European preference' provisions. A number of policymakers and stakeholders have cautioned that a narrow European-preference rule risks hindering European competitiveness and exposing Europe to trade tensions, and Council legal advisers have warned the proposed rules could sit uneasily with the EU's trade commitments. We would encourage a consistent approach across related legal acts, including CADA, to avoid fragmentation and conflicting requirements.

2. DIGITAL OMNIBUS

The Irish Presidency is actively negotiating a compromise on the GDPR and ePrivacy chapters and is heading for a general approach. In Parliament, [Marina Kaljurand \(S&D, Estonia\) leads for LIBE and Aura Salla \(EPP, Finland\) for ITRE](#); they published a joint draft report on 22 June 2026.

The Digital Omnibus was conceived to simplify the EU's digital rulebook, reduce legal uncertainty and unlock investment. The exercise will only be beneficial if it achieves those objectives. A text that reorganises obligations without reducing the complexity created by those requirements will not deliver its intended benefit.

Three areas carry most of the practical value. The first is a workable legal basis for AI. AI models trained on large-scale, diverse datasets cannot be built on individual consent. Legitimate interest, which by definition is a genuine balancing of interests and safeguards, is the legal basis the GDPR provides for precisely such cases. Making that explicit in the operative text establishes a single EU-wide reference point and reduces the risk of divergent national and supervisory readings. But Article 88bis read together with Recital 33a and its reference to consent under national law risks making inoperative the very legitimate interest it claims to confirm, and reopens the fragmentation this file is meant to close.

The second is the definition of personal data. When all data is treated as personal data irrespective of the actual risk of identification, it penalises business for no protective gain and reduces investment in privacy-enhancing technologies and data-driven services. The Court of Justice has confirmed repeatedly, in Breyer and in EDPS v SRB, that information is personal data in the hands of a given entity only where that entity has means reasonably likely to be used to identify an individual. Codifying that principle is one of the most valuable goals the Digital Omnibus could achieve. The workable threshold, that identification is insignificant in practice, has been moved into a recital and belongs in the article.

The third is ePrivacy and the cookie regime. Maintaining two parallel data protection regimes, the GDPR and an ePrivacy Directive dating from a different technological era, is a direct source of fragmentation and compliance cost with no commensurate gain in user protection. The consent-only default for terminal equipment access is also the single largest driver of consent fatigue in Europe, producing click-through rituals that deliver little meaningful protection. Two improvements in the Irish text should be defended: the exemption list has been meaningfully expanded, and the mandatory machine-readable consent signal regime has been deleted. The Council removed Article 88b, which would have pushed consent into browser and operating system settings, on 18 June 2026, and

Parliament may yet restore it. Schemes of this kind were proposed several times in former initiatives and failed for serious legal, technical, economic and anti-trust reasons that are still valid. Moving consent into the browser and the operating system hands one commercially decisive setting to a small number of gatekeepers, and Apple's App Tracking Transparency is the precedent: downstream apps lost an estimated 10 billion dollars in six months while Apple's own services revenue grew, and the French and Italian competition authorities later found the design abusive. Estonian publishers and advertisers would carry that cost with no way to opt out. Separately, returning the storage and access rules to Article 5(3) of the ePrivacy Directive keeps them in a Directive requiring national transposition, outside the one-stop-shop and the consistency mechanism. Twenty-seven transpositions of a single exemption list will preserve the fragmentation the Digital Omnibus is intended to remove.

WHAT WE ASK ESTONIA TO DO

- Preserve Article 88bis in the operative text, where it cannot be diluted into a recital, and remove any reference to consent under national law, in particular in Recital 33a.
- Restore a consolidated recital carrying the beneficial-interest reasoning deleted with recitals 30 and 31, including bias detection and correction, output accuracy, safety and accessibility.
- Put the “insignificant in practice” threshold back in the article, and delete Article 25a(5) or confine it to the recipient's own processing, so that the sender is judged on the situation as it reasonably stood, and on the safeguards it put in place, at the moment of the transfer.
- Confirm in the recitals that pseudonymisation remains a risk-reducing safeguard and that anonymised data falls outside the scope of the Regulation.
- Confirm the deletion of Article 88b and the deletion of the mandatory machine-readable consent signal regime, and retain the expanded exemption list.
- Consolidate the terminal-equipment rules under the GDPR rather than returning them to Article 5(3) ePD, so that a single legal basis framework and a single enforcement architecture apply.
- Judge the result on one question: does a company in Estonia end up with fewer obligations and more certainty than it has today.

3. DIGITAL FAIRNESS ACT (DFA)

Where the file stands: The Commission has said it will propose the DFA in the last quarter of 2026, tabled together with the revision of the Consumer Protection Cooperation Regulation. The KIDS Act, announced on 17 September 2026, took addictive design, profiling-based feeds for minors and age assurance out of the picture, which leaves personalisation and advertising as the centre of gravity of what remains. There is no text yet, which is why Estonia should get its arguments in now.

Fairness is not a legislative problem. The Unfair Commercial Practices Directive and the Consumer Rights Directive already cover false urgency, hidden advertising, fake reviews, interface design and pre-ticked boxes, with Article 28 of the Digital Services Act and now the KIDS Act layered on top. Enforcement already works, as the preliminary DSA findings show, and the 2019 Modernisation Directive updated the UCPD without a *lex specialis*. The real gap is regulatory standards and enforcement capacity, not the mode of regulation. The Commission's own Regulatory Scrutiny Board told DG JUST to refrain from stating or suggesting that the evidence base is robust.

Two ideas in the debate should worry Estonia. The first treats personalised advertising as manipulation. Manipulation already has one definition across the UCPD, the AI Act and the DSA, the material distortion of an autonomous decision, and persuasion is not distortion. The second is dynamic vulnerability, where a consumer's protected status depends on their emotional or financial state at a given moment. Distress cannot be proven in real time, detecting it requires the profiling that the GDPR and ePrivacy restrict, and the resulting identifier becomes a treasure trove for criminals and bad actors. If everyone is vulnerable, vulnerability stops being a legal concept and becomes a reversed burden of proof.

The costs fall on media and advertisers. Independent estimates put compliance and productivity losses at 10.3 to 28.8 billion euros, up to 3.6 times the consumer detriment the DFA addresses, in an EU digital advertising market worth 118.9 billion euros. Advertising is 12.8 percent of broadcasting inputs, so media plurality is directly exposed, and Estonian publishers and retailers have no margin to absorb another layer. The alternative is not what it appears: contextual is not neutral. Proxies replace data, so targeting moves back to postcodes, income, language, gender and ethnicity. Thus, removing digital personalisation does not eliminate discrimination, it launders it through proxies.

WHAT WE ASK ESTONIA TO DO

- Argue for enforcement, not another layer. The EU suffers from judicial and supervisory fragmentation, not legal fragmentation, and that is a question of resources: funding for capacity, and a stronger CPC with mystery shopping, behavioural testing, algorithmic auditing and binding timelines.
- Insist on technologically neutral rules that apply the same test online and offline.
- Reject dynamic vulnerability and keep objective, verifiable criteria.
- Demand a credible impact assessment before the proposal is tabled, covering Estonian media revenues and small advertisers.

4. EU COPYRIGHT DIRECTIVE (EUCD) REVIEW

The European Commission is still assessing feedback it received about the DSM Directive's effectiveness, and its report is due in the nearest months – which is why Estonia should move early, while nothing has been drafted. Meanwhile, the Commission is consulting on plans for a 'targeted' yet far-reaching legislative changes to the EU copyright regime and the European Parliament has adopted non-binding [own-initiative report led by Axel Voss](#), setting expectations in the Parliament.

In the age of AI, the EUCD review is no longer a niche debate between rights holders and AI developers. It is industrial policy for the entire AI value chain, from developers and SMEs to industrial adopters and infrastructure providers. Copyright rules determine which European data is available for AI training and retrieval on European soil, and so decide whether Europe captures or forfeits its AI future. Restrictive, impractical rules could render large-scale training and adoption unviable within the EU and risk years of legal uncertainty and prohibitive costs. A [June 2026 study](#) estimates that tightening the EU's text-and-data-mining framework would put up to 600 billion euros of annual economic value at risk, more than a third of generative AI's 1.7 trillion euro annual potential for the EU.

Data access determines model quality. Quality models rely on training and retrieval-augmented generation on broad and diverse European data, and a larger, predictable European data pool lets developers offer more competitive AI. Europe is already growing world-class labs, with [Mistral raising 3 billion euros at a post-money valuation above 21 billion](#), and for that investment momentum to continue the legal basis for training in Europe

must be secure. A narrower copyright framework directly caps a company's addressable training data, its potential model quality and its long-run competitive position. After the GDPR took effect in 2018, aggregate EU venture deals [fell by around 26 percent](#), and restrictive copyright could repeat that experiment.

Estonian companies should not file this under somebody else's problem. Large industries and SMEs often believe that fine-tuning on proprietary or fully licensed data or using retrieval-augmented generation shields them from the copyright question. In reality they remain shackled to the legal and quality risks inherent in the base model, even where it was trained outside the EU. Past the substantial modification threshold, a manufacturer that merely adapted someone else's model inherits the AI Act's copyright and training-disclosure duties. The Voss report would extend the AI Act's general-purpose AI transparency obligations to downstream deployers and, where training data disclosure is incomplete, presume that protected content was used unless the provider proves otherwise; it also suggests express rights-holder consent for retrieval and inferencing. When rules are opaque and penalties steep, even major enterprises wait or move R&D outside the EU. The quality of a base model dictates the ceiling for all downstream applications, so if models are starved of diverse, high-quality European and Estonian-language data, [Estonian businesses suffer a competitive disadvantage](#) that neither retrieval nor fine-tuning can bridge.

There is also a security dimension that larger Member States do not face in the same way. Estonian is a small language with a correspondingly small body of digital text, and much of the material carrying the country's history, culture and public debate sits in copyrighted archives. If that material cannot lawfully be used for training, models will describe Estonia using whatever sources were available instead, and on many subjects the material available in volume is not Estonian. A restrictive framework does not leave a neutral gap, and an opt-out makes it worse, since the rights holders most likely to withdraw are the ones whose archives would otherwise anchor the record. Ensuring Estonian language and Estonian context are properly represented in the models people actually use is a resilience question.

The second wave of AI is where this bites hardest. While Silicon Valley dominated the first wave, the emerging second wave integrates AI into physical, scientific and industrial sectors such as robotics, manufacturing, engineering, logistics, energy and defence, which leverages Europe's core economic strengths and Estonia's engineering depth. No other region combines a [2.5 trillion euro manufacturing base](#) with equivalent engineering depth and proprietary operational data.

There is an infrastructure paradox as well. The Commission's [30 billion euro AI gigafactory programme](#), including roughly 10 billion in public funding for up to seven sites, risks stalling if

developers take their training demands elsewhere. Europe currently lacks a clear demand signal from developers choosing to train their models locally. True economic AI value for the EU requires ownership of the training process, not just reliance on inference, because that is where the money, the jobs and the strategic export controls are.

WHAT WE ASK ESTONIA TO DO

- Treat the review as industrial policy for the AI value chain, not only as cultural policy.
- Make the case that this is a security and cultural? resilience question as well as an economic one, and raise it in the Council alongside Estonia's cyber and strategic communications work.
- Weigh the full spectrum of choices from restrictive to future-proof, including deleting the ability to opt out of the text and data mining exception, and consider the societal and industrial value of a framework that reflects the reality of how AI systems learn and is aligned with markets where AI technology thrives, such as the United States, Japan, Singapore and Israel. At a minimum, the Article 4 TDM exception must be safeguarded.
- Oppose extending general-purpose AI transparency obligations to downstream deployers, and oppose any presumption that protected content was used where training data disclosure is incomplete.
- Seek clarity on fine-tuning and retrieval-augmented generation, so that Estonian adopters do not become general-purpose AI providers by accident or face pressure to export proprietary data to fine-tune models outside the EU.
- If Europe chooses a more restrictive copyright framework, insist that it does so with full transparency about the economic and societal trade-offs.

WHAT WE ASK IN SHORT

Estonia has used its standing as a digital leader before to push for a positive EU agenda, and it should use it again across these four files, with one line running through all of them: reduce legal uncertainty instead of reorganising it, and preserve the trusted transatlantic partnerships that underpin Europe's digital security and Estonia's own digital success. AmCham Estonia stands ready to continue the dialogue and provide further technical input on any of these files.

