Dear EU Policymakers,

We, the members of ACT | The App Association, are innovative tech small and medium-sized enterprises (SMEs) and independent developers driving growth and competition in the global app economy. From AI-enabled tools, green tech solutions, encrypted services, safer online experiences, and standards-based technologies that enable interoperability, our teams build products that solve everyday problems for communities and customers across Europe.

To continue building, hiring, and scaling across the Single Market, startups and tech SMEs like ours need a regulatory environment that rewards innovation and provides the market certainty required to sustain investment. For tech SMEs, policy volatility quickly becomes a material business constraint that shapes product roadmaps, compliance costs, and go-to-market timelines. Additionally, as roadblocks mount and timelines become harder to predict, investors view the policy environment as an additional risk, often pausing or preventing our access to capital. That is a challenge for European startups and tech SMEs, and a competitiveness challenge for Europe as a whole. A regulatory environment characterised by uncertainty weakens the innovation pipeline Europe relies on to lead in emerging technologies and compete globally.

As policymakers consider new rules for the digital economy, we urge balanced, forward-looking approaches that do not impose disproportionate burdens on tech SMEs, startups, and independent developers. Policy should set clear expectations, provide practical paths to compliance, and deliver durable rules that strengthen trust and security while preserving the conditions that enable smaller innovators to attract investment and compete. Below is an outline of our top policy priorities for EU leadership in 2026.

Market Access and Capital Formation

Scaling across borders is central to the EU growth story for startups, scaleups, and tech SMEs. That requires two conditions that are easy to take for granted until they falter: predictable cross-border data flows, and a credible investment pathway from early-stage funding to scale. For market access and digital trade, cross-border growth depends on stable, workable data transfer mechanisms. When transfer requirements are contested, unevenly interpreted, or operationally burdensome, smaller teams absorb the cost first through slower contracting, higher compliance spend, and more complicated partnerships.

Legal certainty in mergers and acquisitions (M&A) control is critical for capital formation because it determines whether founders, many of whom are serial entrepreneurs, can realistically exit, return capital to early investors, and re-invest that experience and funding into the next company. Over the last few years, shifts in EU merger policy, including a reset of how below-threshold deals are pulled into review and a broader rethink of merger guidelines, reinforce the same lesson: when the rules are unclear or changing, investors price that risk in early, and startups feel it first.

Member Ask: EU policymakers should defend cross-border data flows and prioritise durable, legally certain transfer mechanisms that keep international operations workable for tech SMEs. Policymakers should also implement clear, balanced M&A review processes that distinguish between harmful, anti-competitive mergers and pro-competitive acquisitions that support startup and SME growth.

Unlocking the Single Market

Europe's innovators are building world-class products, but scaling still means navigating 27 different systems for incorporation, regulation, and compliance. The 28th regime and the European Innovation Act should work together to fix that. The 28th regime can reduce structural fragmentation by creating an EU-wide pathway for incorporation and recognition across Member States. The European Innovation Act can reduce day-to-day regulatory drag by building in flexibility for startups to test, iterate, and deploy, through coordinated regulatory sandboxes, innovation stress tests for new legislation, and simpler reporting tools that keep compliance aligned with real-world development cycles.

Member Ask: EU policymakers should deliver a Regulation-based 28th regime that is directly applicable across the EU, not a Directive that recreates fragmentation through 27 national versions. They should also design the European Innovation Act to unlock practical flexibility, including coordinated sandboxes, innovation stress tests, and streamlined reporting, so startups, scaleups, and tech SMEs can build, hire, and scale across the Single Market with legal certainty.

Artificial Intelligence

Tech SMEs are advancing practical AI across Europe, but implementation of the AI Act will determine whether smaller innovators can participate at scale. The AI Act's risk-based approach can work, but only if risk categories are applied clearly and consistently, so everyday tools are not treated like truly high-risk systems. In practice, compliance expectations are also being shaped by overlapping soft-law instruments, including the AI Pact and the General-Purpose AI Code of Practice, which can create early-compliance pressure that favours larger firms. At the same time key technical standards and guidance needed to operationalise the high-risk systems are still under development, creating uncertainty for SMEs. AI adoption challenges also do not exist in isolation.

Member Ask: EU policymakers should implement the AI Act with clear guidance and proportionate obligations that tech SMEs can meet in practice. They should delay the entry into force of the obligations for high-risk AI systems until relevant standards and guidance are finalised, ensure the AI Pact and Code of Practice remain voluntary in practice, and ensure that compliance pathways and support measures are workable for smaller teams building and deploying lower-risk AI tools across the Single Market.

Competition and Privacy

Privacy and competition are deeply interconnected in the EU's digital economy, particularly for startups and small tech. SMEs compete by earning trust, and curated online marketplaces (COMs) help them do so by providing security and privacy tools that smaller teams cannot replicate on their own. The General Data Protection Regulation (GDPR) plays a central role in this ecosystem, but different national interpretations and enforcement uncertainty continue to create compliance burdens for smaller firms that lack in-house legal capacity. At the same time, the implementation of the Digital Markets Act (DMA) and the Digital Services Act (DSA) has created moving compliance targets that first fall on developers, driven by shifting technical requirements, platform changes, and new distribution expectations, which can force mid-cycle rebuilds and disrupt planned launches, including AI-enabled features. When the implementation of the rules keeps changing through guidance and enforcement, it raises costs, increases risk, and makes it harder to scale across the Single Market with confidence.

> **Member Ask:** Policymakers should ensure any EU privacy, security, and competition regulations provide meaningful protections to consumers across the EU while fostering fair competition, without placing undue burdens on SMEs. EU policymakers must prioritise consistent, transparent implementation that reflects the realities of the digital economy and consumer expectations. This includes engaging directly with SMEs to understand their operational challenges and striking a regulatory balance that protects consumer data and intellectual property while supporting small innovators' ability to scale and compete globally.

Standard-Essential Patents (SEP)

Standards can provide the foundation of interoperable technology (Wi-Fi, 5G, Video Encoding), and as AI and the internet of things (IoT) scale, tech SMEs are increasingly building on standards-based ecosystems, including the connected devices and data flows that support many green tech solutions. Over the past few years, the EU's SEP Regulation has also become a moving target. After significant legislative work and political debate, the proposal was ultimately withdrawn, abandoning SMEs to navigate the gauntlet of core challenges to innovation and competition that the European Commission itself painstakingly identified. Unfortunately, some SEP holders who have voluntarily contributed their patents to a standard aren't living up to their commitments. When SEP holders break their promise to license on fair, reasonable, and non-discriminatory (FRAND) terms, it undermines predictable market practices, harms competition, and creates significant problems for small innovators. For tech SMEs that must plan, price, and scale across the Single Market, the exploitation of ambiguities in the EU's SEP licensing framework creates an increasing amount of unnecessary friction and investor hesitation across consumer and enterprise markets.

> **Member Ask:** EU policymakers should restore clarity and accountability while keeping SEP reform moving. We support the European Parliament's decision to pursue judicial review of the withdrawal and urge institutions to uphold transparency and democratic process in EU policymaking. In parallel, EU policymakers should commit to a well-

defined path for reforming the EU's SEP licensing framework that gives startups, scaleups, and tech SMEs the predictability and protection they need.

Encryption

For tech SMEs and independent developers, strong encryption is essential for trusted services and secure communications, which is why the EU's Chat Control proposal matters so deeply to the digital economy. As the file moves into trilogue, the Council position removes the mandatory scanning of encrypted messages, which is essential in preserving end-to-end encryption technology that many applications depend on. We are concerned that risk-mitigation duties could push providers toward surveillance in practice, making age verification and age assessment default expectations, even for services designed to enable private communications. The final text should make it clear that encryption cannot be weakened or bypassed, including through client-side scanning.

> **Member Ask:** EU policymakers should adopt a final text that protects private communications. This should include explicit language ruling out encryption-bypassing measures, such as client-side scanning, and avoid risk benchmarks that turn 'voluntary' detection or intrusive age verification into *de facto* requirements.

Innovation thrives when policymakers create clear, durable rules that allow businesses of all sizes to compete and succeed. Overly broad, fragmented, or unpredictable requirements raise compliance costs, delay product development, and undermine the investment that tech SMEs need to grow. We remain committed to working with the European Parliament, the European Commission, and the Council of the European Union to advance these priorities and ensure that tech SMEs can continue to create jobs and deliver practical solutions in the global digital economy.

Sincerely,

ACT and our members