PRIVACY AND CYBERSECURITY

IMPORTANCE OF PRIVACY AND CYBERSECURITY FOR SMALL APP COMPANIES

Our members care deeply about privacy, understanding that transparency and customer control over data collection and use are essential for building trust and fostering long-term relationships. For example, our members have made substantial investments to comply with the General Data Protection Regulation (GDPR), routinely going beyond its baseline requirements to meet both consumer expectations and competitive market pressures. This includes building in cutting-edge security and privacy features from the earliest stages of product development (privacy-by-design) and using advanced tools such as differential privacy techniques.

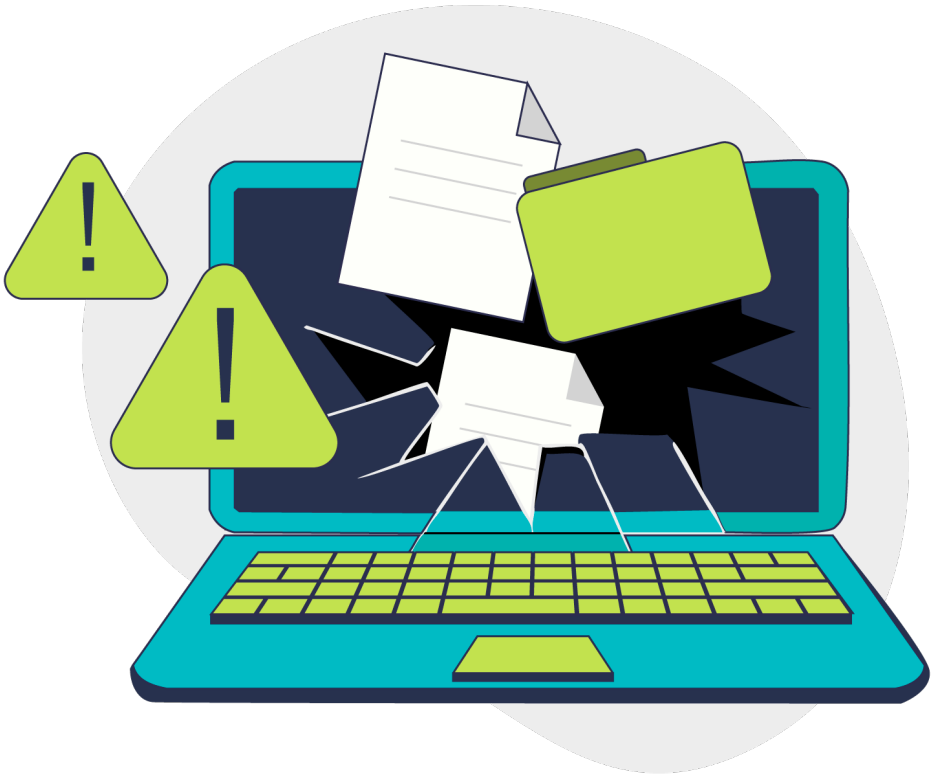
LEGISLATION AND SECURITY

Both consumers and businesses in the UK need a pragmatic and scalable approach to privacy regulation. SMEs require the ability to appropriately tailor their approaches to the needs of their customers and partners, establishing and maintaining consumer confidence. Additionally, we advocate for the development of tools that can assist SMEs in implementing these regulations without compromising their ability to innovate and compete.

However, regulations like the Digital Markets, Consumer and Competition Act (DMCCA) that aren't directly related to privacy or cybersecurity could have sweeping impacts on the security of app ecosystems and consumer trust. The

DMCCA must be implemented in a way that preserves the ability of companies designated as having strategic market status to protect the privacy, security, and intellectual property of users and developers by keeping out bad actors. Failing to do so will allow untrustworthy alternative stores to prey on consumer confusion and erode the trust that SMEs rely on.

SMEs need an ecosystem that supports strong data and privacy protections and maintains robust cybersecurity measures.



THE RISKS OF ENCRYPTION BACKDOORS

The App Association recently wrote to the Home Secretary to raise concerns about the reported Home Office request to create a backdoor into Apple's encrypted iCloud storage services. This would embed a systemic security vulnerability into one of the world's largest mobile device providers, endangering the security and privacy of all its users—not just in the UK, but worldwide. Apple has now discontinued its Advanced Data Protection feature in the UK, reducing the privacy and data security available to UK citizens.

The App Association's small business members both in and outside of the UK know that, in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorised users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorised users. End-to-end encryption is a primary tool for providing trust and security for their customers. Attempts by governments—most recently the UK—to mandate backdoors to encryption algorithms significantly undermines these goals.

UK policymakers must engage directly with SMEs to understand their operational challenges and the policies that protect consumer data and developers' intellectual property while supporting small innovators' ability to scale and compete globally.