Digital Policy Alert

GLOBAL DIGITAL POLICY ROUNDUP

OCTOBER 2026



Global Digital Policy Roundup: October 2026

The roundup is produced by Digital Policy Alert, an independent repository of policy changes affecting the digital economy. If you have feedback or questions, please contact Maria Buza.

POLICY SECTIONS

Content moderation
Artificial intelligence
Competition
Data governance

Overview. The roundup serves as a guide for navigating global digital policy based on the work of Digital Policy Alert. To ensure trust, every finding links to the Digital Policy Alert entry with the official government source. The full Digital Policy Alert dataset is available for you to access, filter, and download. To stay updated, Digital Policy Alert also offers a customizable notification service that provides free updates on your areas of interest. Digital Policy Alert's tools, such as the MCP and Clairk, further allow you to navigate, compare, and chat with the legal texts of digital rules across the globe.

Drawing on Digital Policy Alert's daily monitoring of developments in over 60 jurisdictions, the roundup summarizes the highlights of October 2026 in four core areas of digital policy:

- **Content moderation,** including Turkey's regulation requiring social network providers to verify users' ages and bar children under 15, Mexico's decree on safe digital environments for children and adolescents, the introduction of Australia's Digital Duty of Care Bill, and the European Commission's formal proceedings against Booking under the DSA.
- **Artificial intelligence,** including the European Commission's consultation on procedural rules for AI Act enforcement, Italy's Legislative Decree designating its national AI Act authorities, the EU–Canada joint statement on AI safety and governance, China's consultation on adding 23 AI technologies to its export control framework, and Japan's establishment of the AI and Digital Reform Promotion Council.
- **Competition,** including South Korea's ₩42.9 billion and ₩20.81 billion fines against Google and Apple over in-app payments, the Competition and Markets Authority's proposed designation of Microsoft as having strategic market status in business software, Türkiye's investigation and interim measures on Google's AI Overviews and AI Mode, Poland's commitment decision requiring Apple to show neutral App Tracking Transparency consent notices, and the entry into force of Russia's platform economy law.
- **Data governance,** including the Council of the EU's position on the Digital Omnibus, France's €7 million fine against Fnac companies over app trackers, the entry into force of South Korea's amended Network Act incident reporting rules, the introduction of Vietnam's draft Data Security Law with tiered cross-border transfer rules, and Canada's Children's Privacy Code.

Content moderation

Europe

In the **European Union**, the European Commission continued enforcing the Digital Services Act (DSA). It opened formal proceedings against Booking to assess its compliance with obligations to mitigate fraud and phishing risks, including fake property listings and impersonation fraud, and to identify listings promoted through higher commissions as advertisements. The Commission also approved Temu's action plan to address its breach of risk assessment obligations concerning the sale of illegal products, following a €200 million fine imposed in May 2026. Temu has four months to implement five corrective measures, which an independent external auditor will assess. The Commission also published a study on financial scams on online platforms to inform its supervisory activities. The study examines platform features exploited by scammers, including advertising, recommender systems, fake accounts and generative AI, as well as potential countermeasures, such as know-your-business-customer checks, scam detection and removal mechanisms, and user reporting tools. At the judicial level, the General Court upheld the designation of Stripchat as a very large online platform, dismissing Technius' challenge to the user data used by the Commission as the basis for the designation.

At the **member-state level**, the Greek Parliament adopted a bill restricting access to social networking services for minors under 15, with age verification through the digital document repository or the "KidsWallet" application. In Hungary, a bill was introduced to Parliament to require high-risk platforms to verify users' ages, restrict access for children under 13, and limit access for those under 16 to private-by-default accounts and adjusted recommender systems. In Belgium, the Federal Government introduced a bill partially implementing the EU Product Liability Directive, extending the definition of products to software and digital manufacturing files and liability to online platforms presenting products as their own.

In **France**, the Regulatory Authority for Audiovisual and Digital Communication (Arcom), the national Digital Services Coordinator under the DSA, opened an investigation into Mym, a social network offering exclusive and personalized content, often of an erotic or sexual nature, over alleged non-compliance with the DSA. The investigation will examine the platform's measures to protect minors as well as the transparency of its terms of use and recommender systems.

In **Germany**, the Federal Cabinet approved the draft bill that would allow people whose personality rights are violated online to obtain user information from platforms by court order, and would let courts order account suspensions. It would also create new criminal offenses for the unauthorized creation and distribution of intimate images, including sexualized deepfakes. A bill to guarantee freedom of expression in social networks was introduced to Parliament, which would remove DSA liability exemptions for social networks that carry out voluntary investigations beyond removing illegal content. Finally, the Federal Court of Justice referred questions to the Court of Justice of the European Union concerning social network operators' liability for user-posted false statements, including whether algorithmic content curation affects their status as hosting services under the DSA and whether they can be required to manually review equivalent content.

In **Russia**, the Law on platform economy harmonization (290-FZ) entered into force, extending intermediary digital platform operators' liability for losses caused by inaccurate or incomplete information and requiring platforms to facilitate consumer claims and refunds. The Law also

restricts the offering of certain non-compliant goods and introduces registration, notification, and compliance requirements for foreign platforms meeting specified user thresholds.

In **Switzerland**, the Federal Council reviewed the consultation results on the draft Federal Law on Communications Platforms and Search Engines and instructed the preparation of a revised draft for submission to Parliament by June 2027. The revised draft would require platforms to accept reports of all content suspected of being unlawful, notify users of content removals and account restrictions, explain their decisions and provide complaint mechanisms. It would also introduce measures to protect minors, including a ban on profiling-based advertising to minors.

In **Turkey**, the Cyber Security Directorate of the Presidency adopted the regulation on differentiated services for children and age verification by social network providers, which enters into force on Nov. 1, 2026. The regulation requires providers to verify users' ages at account creation to prevent children under 15 from accessing their platforms, with existing accounts to be verified by March 31, 2027. For users aged 15 to 17, providers must offer differentiated services, including content filtering, recommender system settings to reduce exposure to harmful content, and an appeal mechanism subject to meaningful human review. Child accounts must be private by default, with live streaming, addictive features, and sequential content feeds disabled, and parental control tools provided. Additionally, two bills were introduced in the Grand National Assembly. The first bill would introduce age verification, parental consent, daily screen-time limits of 55 minutes for users under 16, and a ban on access to digital media and devices between 10:30 p.m. and 9:30 a.m., with educational content exempt. Game companies would have to apply the same 55-minute limit to online games, and gambling operators would have to block access for users under 18. It would also require platforms to provide parents with usage reports and alerts about risky content. Breaches, other than those concerning the time-limit mechanisms and parental reports, could result in administrative fines of ₺1 million to ₺5 million. The fine would increase by half for a second repeat offense within one year, and a third would lead to the termination of the provider's activities. Digital content providers would have six months from entry into force to comply. The second bill, which includes measures to combat violence against women, would require platforms to remove non-consensual intimate content and deepfakes within four hours of notification, address other notices concerning violent content within 24 hours, and respond to emergency requests from trusted flaggers within two hours. Violations could result in fines of up to ₺200 million and bandwidth restrictions of up to 90% for systematic non-compliance.

In the **United Kingdom**, the Office of Communications (Ofcom) amended its Illegal Content and Protection of Children Codes of Practice, requiring certain user-to-user services to establish internal crisis response procedures for events posing serious risks to public safety. The requirements apply to services with more than 7 million monthly active UK users at medium risk and to services of any size at high risk. Ofcom also issued its assessment regarding age assurance methods for the planned social media ban for under-16s, identifying photo ID, digital ID, banking-based checks and facial age estimation as methods that can meet the required standard.

Regarding **enforcement**, Ofcom opened an investigation into Meta over its alleged failure to conduct illegal content and children's risk assessments before launching Instagram's Instants feature. It also narrowed its investigation into X to illegal content and complaints-handling obligations, dropping the age assurance aspect following changes to the service. Separately, Ofcom opened an investigation into an adult image-hosting service over its alleged failure to protect users from non-consensual intimate imagery, including through hash-matching technology.

At the **judicial level**, the High Court dismissed judicial review claims brought by X, TikTok and Meta and WhatsApp against Ofcom's information notices under the Online Safety Act. The notices require the platforms to provide data on content moderation measures, the reach of moderated content, and user complaints and appeals.

Asia and Australia

In **Australia**, the Online Safety Amendment (Digital Duty of Care) Bill was introduced in the House of Representatives. It would replace the Basic Online Safety Expectations with a statutory digital duty of care, requiring online service providers, including services that enable users to generate content using AI, to take appropriate measures to ensure online safety. For users under 16, social media services would have to ensure that design features associated with negative behavioral impacts, including recommender systems, endless feeds, engagement metrics and ephemeral content, are not available. The Bill would also shorten the deadline for platforms to act on cyberbullying and cyber-abuse complaints from 48 to 24 hours before the eSafety Commissioner could issue a removal notice, and empower the Commissioner to order the removal of apps and websites designed to generate fake nude images. Additional provisions would allow the Minister to require services to provide user empowerment tools and expand the Commissioner's information-gathering and transparency reporting powers.

Regarding **enforcement**, the eSafety Commissioner published a transparency report on Roblox, Minecraft, Fortnite and Steam under the Basic Online Safety Expectations. The report identified differences in the use of proactive detection tools, noting that Valve was the only provider not using hash-matching technology, while Minecraft and Fortnite relied primarily on self-declared age. The Commissioner is seeking commitments from Valve to introduce additional age assurance methods.

In **India**, the Supreme Court directed the Union Government to implement a framework for the detection, removal and reporting of child sexual exploitation and abuse material by intermediaries. Further, the Court declined to endorse an age-based social media ban, holding that internet access is a fundamental right of children.

Regarding **enforcement**, the Central Consumer Protection Authority (CCPA) fined Meesho ₹1 million for facilitating the sale of an unregistered herbicide and Just Dial ₹1 million for listing and facilitating the sale of ammonium nitrate. The CCPA also fined Hogar Technologies and Innovations ₹100,000 for misleading advertisements for walkie-talkies and directed Agoda to prominently display its grievance officer's contact details. It also closed its investigations into Amazon and Flipkart over alleged deceptive pricing without imposing penalties.

In **Malaysia**, the Communications and Multimedia Commission (Amendment) Act entered into force, expanding the Commission's mandate to cover interoperability, trust, security and integrity standards for communications infrastructure and platforms, as well as audits of licensees and other service providers.

Regarding **enforcement**, the Communications and Multimedia Commission reported Meta's response regarding WhatsApp account suspensions. Meta attributed more than half of the cases to a technical error, which it stated had been resolved. The Commission requested improvements to Meta's appeal and account recovery processes and indicated that further regulatory action could follow if the measures were inadequate.

In **South Korea**, the grace period ended for e-commerce operators to comply with review-disclosure requirements, including disclosure of review eligibility, rating criteria, and procedures for contesting review removals. The Fair Trade Commission also issued guidelines covering 13 types of dark patterns and prohibited practices under the Act on Consumer Protection in Electronic Commerce, including drip pricing, pre-selection, and obstruction of cancellation. Meanwhile, the Broadcasting, Media and Communications Commission launched the Information and Communications Service Transparency Center to support fact-checking and verify transparency reports submitted by large service providers under the amended Network Act. Additionally, two bills were introduced in the National Assembly. A bill amending the Network Act would require large social media providers to verify users' ages and prohibit personalized recommendations on minors' accounts. A bill amending the Telecommunications Business Act would extend operators' obligations to remove or block illegally filmed material to victims' personal information and prohibit the misuse or disclosure of reporters' personal information, with penalty surcharges of up to 3% of sales.

Regarding **enforcement**, the Fair Trade Commission imposed a provisional fine of ₩20.114 billion and issued a corrective order against Samsung Electronics over advertising the gaming performance of its Galaxy S21, S22 and Tab S8 devices that did not disclose processor speed restrictions imposed by its Game Optimizing Service.

In **Thailand**, the Office of the Consumer Protection Board opened a consultation on a draft bill amending the Direct Sales and Direct Marketing Act to cover sales through digital platforms and social media. The bill would expand the definition of direct marketing to include e-commerce and digital platform services, require platforms to collect seller information, and introduce a 14-day right to cancel contracts. It would also make digital platforms jointly liable with sellers for defective goods.

Americas

In **Argentina**, the Secretariat of Industry, Commerce and SMEs signed an agreement with Meta to remove reported Facebook and Instagram pages suspected of facilitating the sale of illegally imported goods.

In **Brazil**, the ordinance on paid advertising and content amplification entered into force. It requires internet application providers to store advertising information for at least one year, and those with more than one million monthly active users to maintain a public advertisement repository. Content creators must disclose material relationships with advertisers, and providers must verify advertisers of financial products and services. The National Consumer Secretariat (Senacon) may access the retained advertising data when investigating consumer protection infringements. On child protection, the Federal Police's ordinance on reporting child sexual exploitation and abuse content entered into force. It requires services directed at or likely to be accessed by children, as well as pornographic and escort services, to register in the Nidus System. The President also adopted a Decree on consumer service channels under the Consumer Protection Code. It sets quality of service requirements, such as free 24/7 channels, access to a human agent, and immediate cancellation. It also requires digital intermediation, ride-hailing, and delivery platforms to submit their consumer service models to Senacon for assessment. Meanwhile, the Chamber of Deputies' Committee on Industry, Commerce and Services approved a bill that would allow establishments on delivery applications to set minimum order values, provided these are disclosed before purchase.

Regarding **enforcement**, several authorities examined Meta's content moderation practices. The Federal Public Prosecutor's Office for Citizens' Rights opened an administrative procedure into Meta after more than 1,000 reported account suspensions during the electoral period. The Federal Public Prosecutor's Office filed a lawsuit seeking the reinstatement of student organizations' Instagram profiles. The National Data Protection Agency opened an inspection into how Meta suspends accounts, restricts reach, and removes content, including how it reviews automated decisions after user appeals.

At the **judicial level**, the Superior Electoral Court ordered Meta to apply identical distribution, recommendation, advertising, and Meta AI criteria to both candidates in the presidential runoff. After finding that Meta had not satisfactorily complied, the Court ordered it to prove compliance or face a daily fine rising from R$500,000 to R$1 million. Separately, the Labor Court of São Paulo ordered Meta to remove, within 24 hours, 14 posts alleged to constitute electoral harassment in the workplace, and to display a notice to users stating that such harassment is prohibited.

In **Mexico**, the Government adopted a Decree on safe digital environments for children and adolescents, which entered into force without a grace period. It requires platforms, including social networks, video games, and app stores, to prevent minors from accessing or being recommended harmful content. This covers harassment, sexual abuse, hate speech, pornography, suicide, self-harm, and eating disorders. Platforms must also remove such content and provide reporting mechanisms. Further, platforms must use age verification that does not rely solely on self-declaration and build safeguards into service design, including parental supervision tools and strict default settings, and regularly assess the risks arising from their design and recommender systems.

Africa

In **Egypt**, the 30-day deadline expired for social media platforms to submit implementation plans under the Joint Resolution on the protection of children and adolescents on social media. The Resolution restricts account creation for children under 13 and requires a default "safe mode" for those aged 13 to under 15.

In **Nigeria**, the Federal Competition and Consumer Protection Commission consulted on the Draft Sales Promotion (Amended) Regulations. The draft would extend the rules to promotions run through apps, social media and e-commerce platforms. It would require transparent algorithmic targeting, disclosure of paid influencer relationships, and labels on AI-generated marketing. Platforms and influencers would share liability with promoters for misleading promotions, with fines of up to ₦50 million for individuals and ₦100 million or 1% of prior-year turnover, whichever is greater, for companies.

Artificial intelligence

Europe

The **European Commission** opened a consultation on a draft Implementing Regulation setting procedural rules for its enforcement proceedings under Articles 75c and 75d of the AI Act. The rules would apply to AI systems the Commission supervises directly. These include systems built on a general-purpose AI model by the same provider, and systems that form part of very large online platforms or search engines. The draft would also set out when the five-year limitation

periods for imposing and enforcing fines begin, and when they are interrupted or suspended. Separately, the harmonized standard on quality management systems for the AI Act became applicable after its publication in the Official Journal. The standard sets requirements for providers of AI systems, mainly high-risk systems, to establish and maintain a quality management system, including post-market monitoring, across all sectors.

At the **bilateral level**, the European Union and Canada adopted a joint statement committing to cooperate on AI safety, security and international governance, and to seek compatibility between their digital rules.

At the **member-state level,** Finland's Government submitted a bill to align its national AI supervision act with the AI Act and the Digital Omnibus on AI. The bill would require the Transport and Communications Agency to set up a national AI regulatory sandbox, and would introduce a notification obligation for high-risk AI systems linked to critical infrastructure. In Poland, the provisions of the Act on Artificial Intelligence Systems on inspections, enforcement proceedings and penalties under the AI Act became applicable. These include a settlement mechanism that allows reduced fines. In Belgium, a bill was introduced to Parliament that would presume that providers of AI models or systems have used copyright-protected works where evidence from the system's development, deployment or output makes such use likely.

In **Italy,** the President adopted a Legislative Decree implementing the AI Act, which designates the Agency for Digital Italy (AgID) as the notifying authority, and the National Cybersecurity Agency as the market surveillance authority and single point of contact. The decree also sets fines of up to €35 million or 7% of turnover and creates an AI regulatory sandbox run by AgID and the National Cybersecurity Agency. Financial sector supervisors and the Data Protection Authority act as market surveillance authorities within their remits. It also requires employers that use AI in employment decisions to ensure a natural person makes final decisions on hiring, changes to employment, and dismissal, and gives workers a right to an explanation. In addition, it protects the data, algorithms and mathematical methods used to train AI systems as trade secrets.

Regarding **enforcement**, the Competition Authority opened a consultation as part of its unfair contract terms investigation into Suno's AI music service. The consultation covers terms of service clauses that allow unilateral changes to terms and prices, limit liability broadly, and grant a perpetual, royalty-free license over user content.

In **Russia**, two three-year experimental legal regimes for autonomous systems entered into force. Resolution No. 1247 covers delivery rovers in 34 constituent entities and sets technical requirements, speed limits, data transmission duties, and liability insurance requirements. Resolution No. 1259 covers highly automated equipment at six airports and requires remote monitoring, manual control in the event of faults, and compliance with information security requirements.

In the **United Kingdom**, the Law Commission of England and Wales opened a consultation on its review of product liability law. It provisionally proposes that software and AI systems count as products, whether embedded in physical items or delivered digitally, and asks whether AI models should qualify as products on their own. The Information Commissioner's Office (ICO) opened a call for evidence on how data protection law applies to agentic AI systems. It also published a report setting out its expectations for foundation model developers on transparency, lawful basis and data subject rights.

Regarding **enforcement**, the Intellectual Property Office refused a patent application by Emotional

Perception AI for a trained neural network that recommends similar music files. The decision followed the Supreme Court's remittal of the case. The Office held that the claimed benefit was purely subjective and that the invention lacked an inventive step.

Asia and Australia

In **China**, the Ministry of Commerce and the Ministry of Science and Technology opened a consultation on amendments to the export control framework that would add 23 AI technologies relating to large-scale models, intelligent agents, computing clusters and information processing, as well as 12 photovoltaic technologies. It would also introduce temporary pre-export registration requirements and would exclude open-source AI technologies. The Cyberspace Administration of China published the nineteenth batch of its deep synthesis algorithm filing list. The registry now holds 842 algorithms for generating text, images, video, audio, digital humans and multimodal content.

In **Indonesia**, the Ministry of Communication and Digital Affairs announced it is assessing a ministerial regulation that would require AI developers to label video and other digital content generated by their products. It is considering an approach based on content authentication and provenance metadata.

In **Japan**, the Cabinet established the AI and Digital Reform Promotion Council to coordinate government work on AI and digital transformation. Its first meeting will address the revision of the guidelines on trustworthy AI, a possible revision of the AI Promotion Act, liability for AI agents and physical AI, and government oversight of advanced AI capabilities. Following a large-scale data leak at telecommunications providers, the Ministry of Internal Affairs and Communications also established a study group on data protection and security in telecommunications services in the frontier AI era.

In **South Korea**, the Fair Trade Commission opened a consultation on proposed guidelines on labeling and advertising related to AI. The guidelines address "AI washing" by requiring businesses to substantiate AI-related claims and to provide clear labels on AI-generated virtual persons used in endorsements. Several bills were also introduced to the National Assembly. A bill amending the Network Act would require generative AI chat services to show excessive-use alerts to minors and offer tools to limit their usage time. A bill on intelligent robots would establish a Robot Industry Strategy Committee, a framework for robot training data and an Intelligent Robot Ethics Charter, and would make safety certification and insurance mandatory for intelligent robots, including humanoid robots. A bill on industrial digital transformation would provide for a three-year industrial AI plan, pilot zones for testing and certifying industrial AI products, and an industrial data library with graded security measures. Two bills would amend the Special Act on Promotion of AI Data Center Industry. The first would require operators building or expanding large AI data centers to obtain local government permits after reviewing the impact on residents and disaster safety. The second would remove the provision that deems certain building permits granted for AI data center projects, and would require local electricity self-sufficiency to be considered when designating AI data center special zones.

Vietnam and Japan agreed on an implementation plan for their memorandum of understanding on ICT and digital transformation. The plan covers programs on AI, large language models and AI governance, and the joint development of Vietnamese-language AI models.

Americas

Canada and the United Kingdom renewed their bilateral cooperation on AI security, under which the Canadian AI Safety Institute and the UK AI Security Institute will jointly develop interoperable AI security standards, share information on AI security through Five Eyes mechanisms, and hold recurring technical discussions on the capabilities and risks of the most advanced AI models, including possible joint testing exercises.

Regarding **enforcement**, the Office of the Information and Privacy Commissioner for British Columbia announced an investigation into OpenAI over its use of personal information in delivering ChatGPT responses, following media reports linking ChatGPT to events preceding a shooting in Tumbler Ridge. OpenAI petitioned the Supreme Court of British Columbia for judicial review of the Commissioner's order compelling it to produce information.

Africa

The Bank of **Ghana** opened a consultation on the draft Credit Risk Management Directive, which would permit automated credit decision tools only under set conditions, including explainable models, bias monitoring, independent validation, and a borrower right to request human review. Regulated financial institutions would also need a governance framework for AI in credit risk management, with human oversight and annual reporting on material AI models.

Competition

Europe

The Council of the **European Union** adopted the Decision concluding the EU–UK Competition Cooperation Agreement, establishing a framework for cooperation between their competition authorities. The EU and Canada concluded negotiations on a second-generation agreement providing for cooperation on cross-border competition investigations and information exchange, subject to legal safeguards.

At the Court of Justice of the European Union, the Advocate General recommended dismissing the examined parts of ByteDance's appeal against TikTok's gatekeeper designation under the Digital Markets Act. The opinion found that companies must offer strong arguments to rebut the gatekeeper presumptions, and that users' activity on rival social networks does not on its own disprove TikTok's role as a gateway.

At the **member-state level**, Denmark's Competition and Consumer Authority carried out unannounced inspections in the digital platform intermediation sector over suspected anti-competitive agreements. In Poland, the Office of Competition and Consumer Protection (UOKiK) issued a binding commitment decision requiring Apple to show neutral consent notices under its App Tracking Transparency Framework, applying equally to its own and third-party apps. The decision removes wording such as "tracking" that may have discouraged users from sharing data with third-party publishers and favored Apple's own advertising services. UOKiK also opened an abuse-of-dominance investigation into Google over its remuneration negotiations with Polish press publishers. According to UOKiK, Google had proposed rates without providing the legally required information on how it uses press publications, the revenue they generate, and how it calculated the rates.

In **Russia**, Federal Law No. 289-FZ regulating the platform economy entered into force, setting rules for relations between intermediary digital platform operators, their partners, and users. The Law sets requirements on equal access, non-discrimination, transparency, contract terms, search ranking, price discounts, and complaints, and creates a unified register of intermediary digital platforms.

In **Switzerland**, the Federal Council opened a consultation on an amendment to the Federal Act against Unfair Competition that would require payment service providers to disclose service commissions, interchange fees and scheme fees for cashless payments to merchants.

In **Turkey**, the Competition Authority opened an investigation into Google over alleged abuse of dominance through its AI Overviews and AI Mode features, examining their impact on news publishers' traffic and content agreements. The Competition Board also imposed interim measures requiring Google to ensure non-discriminatory content-use conditions that reflect the economic value of publishers' content and allow them to opt out without affecting their visibility on other Google services.

In the **United Kingdom**, the Competition and Markets Authority (CMA) opened a consultation on a proposed conduct requirement that would oblige Apple to give developers access to near-field communication technology on iOS devices on fair, reasonable, transparent, and non-discriminatory terms, and to allow users to set a third-party app as their default contactless app. Additionally, the CMA opened a consultation on its proposed decision to designate Microsoft as having strategic market status in business software, including its PC and server operating systems, productivity suite, database software, and security software. The CMA provisionally found that Microsoft holds substantial and entrenched market power and does not expect cloud adoption or AI to erode it over the next five years. Finally, the CMA opened an investigation into whether Meta abuses a dominant position through terms that could let it reuse content from businesses' websites for its own products, including AI tools. Meta has suspended the terms while it consults industry groups.

Asia and Australia

In **Japan**, the Fair Trade Commission launched a survey of 50,000 companies on compliance with its guideline on abuse of superior bargaining position, which addresses acquiring intellectual property, know-how, and data from smaller partners without adequate compensation. The Commission plans to send warning letters where responses point to practices that may raise competition concerns.

In **Malaysia**, the Ministry of Communications announced an inquiry into the effects of e-commerce platforms on small and medium enterprises, the retail sector, and the postal and courier industry, following traders' concerns over products sold below market prices.

In **South Korea**, a bill introduced to the National Assembly would amend the Telecommunications Business Act to let operators under investigation for prohibited acts propose voluntary corrective measures through a consent decree. The bill would also allow the Broadcasting, Media and Communications Commission (BMCC) to close cases without ruling on illegality.

Regarding **enforcement**, the BMCC fined Google ₩42.9 billion and Apple ₩20.81 billion and issued corrective orders for forcing developers to use their in-app payment systems, in its first enforcement action under the 2021 amendment to the Telecommunications Business Act on app

market operators. The BMCC found that both companies prohibited external payment, charged a 26% commission on third-party payments, and delayed app reviews without justification, and that Apple discriminated between domestic and foreign developers in applying its commission. The fines followed the BMCC's clarification, in response to media reports, that its deliberations were still ongoing.

In **Thailand**, the Office of the Trade Competition Commission opened a consultation on a draft regulation that would classify ride-hailing and on-demand delivery platform services as essential facilities, with fees charged to drivers and merchants required to be cost-based, itemized, and fair, reasonable, and non-discriminatory. Operators with market power would have to notify fee increases 90 days in advance, while dominant operators would need prior approval from the Trade Competition Commission.

Africa

In **South Africa**, the amended Rule 39 of the Competition Commission Rules entered into force, setting a new procedure for addressing breaches of merger conditions through a Notice Requesting Compliance and remedial plans. The Minister of Communications and Digital Technologies issued a Policy Direction on electronic communications network deployment.

Regarding **enforcement**, the Competition Commission recommended unconditional approval of the acquisition of vacant industrial land in Brackenfell by Teraco Properties, which is controlled by data center operator Teraco and ultimately by Digital Realty Trust.

Data governance

Europe

In the **European Union**, the Implementing Regulation establishing 27 minimum metadata elements for electronic health datasets used for secondary purposes entered into force. Health data holders are required to apply them from March 2029 under the European Health Data Space Regulation. Additionally, the Council agreed its position on the proposed Digital Omnibus Regulation. On data protection, it would keep the General Data Protection Regulation (GDPR) definition of personal data while clarifying measures on pseudonymization and identifiability, and allow sensitive data to be processed for biometric verification and for developing and operating AI systems subject to safeguards. On data sharing, it would repeal the Regulation on the free flow of non-personal data, move its ban on data localization requirements into the Data Act, and limit business-to-government data sharing under the Data Act to public emergencies. On cybersecurity, member states would have to set up national single entry points for incident reporting instead of the Union-wide entry point proposed by the Commission. On governance, GDPR authorities would supervise the Data Act in matters concerning personal data, and the European Data Innovation Board would retain its advisory role. Separately, the European Data Protection Board adopted a statement on smart glasses with preliminary guidance on data protection risks for users, manufacturers, and providers of linked apps, including AI services, and called for safeguards to inform bystanders.

At the **member-state level,** Bulgaria's Personal Data Protection Commission adopted a regulation

on accrediting GDPR certification bodies and a regulation on accrediting bodies that monitor codes of conduct. Germany's Bundestag adopted the Act implementing the EU Cyber Resilience Act, which makes the Federal Office for Information Security the market surveillance and notifying authority, with powers to check IT products, impose fines, and withdraw non-compliant products. In the Netherlands, the Authority for Consumers and Markets opened a consultation on draft guidelines on switching between cloud and other data processing services under the Data Act. In Poland, the Council of Ministers adopted a proposal for the Act on fair access to and use of data, which would designate the President of the Office of Electronic Communications as the authority supervising the EU Data Act.

Regarding **enforcement**, Croatia's Personal Data Protection Agency fined a gambling operator €2.59 million for collecting excessive biometric data without valid consent. Finland's Data Protection Ombudsman fined Mindemo Oy €33,000 for passing users' therapy appointment data to Google, Meta, and Microsoft through website trackers. In the Netherlands, the Data Protection Authority concluded an inquiry into debt collection agencies' use of algorithms and AI, finding insufficient safeguards and recommending meaningful human involvement in significant decisions and more transparency toward debtors. It also opened an investigation into two organizations whose cookie banners still lacked a directly visible reject button, after warning around 100 organizations.

In **France**, the National Commission on Informatics and Liberty (CNIL) fined Fnac Darty Participations et Services and Fnac Direct a total of €7 million for sending user identifiers and browsing activity in their app to a third party without consent, in breach of the national rules implementing the ePrivacy Directive. The entities must show the regulator within one month that they obtained consent where required, or face a penalty of €10,000 for each day of delay.

In **Switzerland**, the Federal Administrative Court confirmed that PostFinance needs explicit consent to create customer voiceprints, which are biometric data, and gave it until mid-February 2027 to obtain consent for existing voiceprints or delete them. The Federal Data Protection and Information Commissioner opened an investigation into pension software provider PK Softech AG after a cyberattack in which data from several pension institutions was extracted.

In the **United Kingdom**, the Information Commissioner's Office (ICO) adopted guidance on data protection by design for designers of Smart Data schemes, which let authorized third parties access customer data under the Data (Use and Access) Act. The ICO also revised its guidance on special category data to reflect the Act. HM Treasury published the Data Centre Covenant, setting five conditions, including security and cyber resilience commitments, for government support to strategic data centers.

Regarding **enforcement**, the ICO reprimanded Ogi Networks and the Local Government Data Unit – Wales for breaching UK GDPR security rules after a ransomware attack, enabled by a test account with a very weak password, exposed the personal information of 3,300 people, mostly children. The First-tier Tribunal approved an agreement ending DSG Retail's appeal, under which DSG will pay £200,000 of the penalty imposed over a 2017–2018 cyberattack affecting around 5.6 million payment cards.

Asia and Australia

The Office of the **Australian** Information Commissioner announced an investigation into Shenzhen

Qingcheng Future Technology, developer of the HeyCyan app used by many smart glasses sold in the country, after the company did not respond to inquiries on how the glasses record and store information. The Commissioner urged retailers to consider whether to keep selling the devices.

In **China**, the Ministry of Industry and Information Technology ordered the developers of 17 mobile apps and software development kits to fix infringements, including illegal collection of personal information, excessive permission requests, and forced personalized recommendations.

In **India**, a lawsuit was filed at the Supreme Court challenging the constitutionality of the Digital Personal Data Protection Act, 2023, and its 2025 Rules, including provisions on processing without consent for legitimate uses, government exemptions, the Data Protection Board's powers, and the amendment to the Right to Information Act. The petitioners have asked for a stay.

Indonesia's Ministry of Communication and Digital Affairs announced an investigation into the alleged illegal trading of personal data on websites and digital platforms, together with the National Police and the National Cyber and Crypto Agency.

In **Japan**, the Personal Information Protection Commission (PPC) presented basic policy considerations for implementing the amended Act on the Protection of Personal Information. It covers administrative surcharges for improper use, improper acquisition, or unlawful third-party provision of personal data affecting more than 1,000 individuals, and rules on contactable personal-related information, such as cookie IDs and advertising identifiers, and on the opt-out system used by list brokers. The PPC also issued an alert on responding to large-scale data leaks with revised technical security measures, such as phishing-resistant multi-factor authentication, while the Financial Services Agency issued an alert asking financial institutions for stricter remote identity checks after leaks of customer identification documents.

In **Malaysia**, the Personal Data Protection Department consulted on the draft AI and Personal Data Protection Framework, which would require data controllers using AI to disclose it in privacy notices, apply data protection by design and pre-deployment testing, conduct due diligence on AI providers, and assess AI systems for bias.

In **New Zealand**, the National Cyber Security Centre issued a security alert on two critical, reportedly exploited PHP vulnerabilities that could let attackers run code remotely without logging in.

Regarding **enforcement**, the Office of the Privacy Commissioner published its final report on the investigation into the cybersecurity breach of the Manage My Health patient portal, finding that the operator violated the Health Information Privacy Code by importing hospital information without a valid purpose or patient consent and by keeping inactive accounts for 24 months.

In **Saudi Arabia**, the Saudi Data and AI Authority opened a consultation on amendments to the Implementing Regulation of the Personal Data Protection Law. The proposed amendments would require controllers to report all personal data breaches within 72 hours, extend impact assessments to minors' data and large-scale processing, and require consent for promotional messages even where a prior relationship exists.

In **Singapore**, the Minister for Home Affairs announced enhancements to the National Cybersecurity Command Centre, including a national service blocking known malicious domains,

monitoring of critical information infrastructure owners' internet-facing systems, and AI-enabled incident response coordination.

In **South Korea**, incident response rules in the amended Network Act entered into force, requiring information and communications service providers to appoint an executive Chief Information Security Officer, report cybersecurity incidents to authorities within 24 hours, and notify affected users without delay. Amended Standards for Measures to Ensure the Safety of Personal Information on internal management plans, access control, unauthorized access prevention, and access log retention also entered into force. Further, two bills were introduced to the National Assembly: one would amend the Act on Consumer Protection in Electronic Commerce to allow online sales intermediaries to share consumer transaction records and personal information with vendors with consumer consent, and the other would amend the Personal Information Protection Act to create a compensation fund for victims of data leaks.

The Personal Information Protection Commission (PIPC) adopted a plan to strengthen investigations into data leaks, setting processing time goals and allowing a 40% surcharge reduction for effective incident response. The PIPC also issued guidance on preventive measures against AI-enabled hacking and on data leaks linked to the PHP2Shell vulnerability, while the Ministry of Science and ICT (MSIT) and the Korea Internet and Security Agency issued a security advisory on the PHP vulnerabilities and raised the private-sector cyber crisis alert to "Caution." The PIPC announced a review of whether the United Kingdom offers substantially equivalent data protection, which would allow transfers without additional requirements, and opened a consultation on amending its Supplementary Rules for data transferred from the EU, following the European Commission's review of its adequacy decision.

Regarding **enforcement**, the PIPC fined Daekyo ₩3.255 billion for failing to implement safety measures after breaches leaked the personal information of about 650,000 users of its online education service. The MSIT announced a joint public-private investigation into a security breach at enterprise software provider Douzone Bizon, including possible spillover to client companies.

In **Thailand**, the Personal Data Protection Committee published non-binding guidelines on personal data protection in the development and use of AI, covering data controllers, processors, AI developers, and deployers. The guidelines state that prompts, usage logs, and AI outputs may be personal data, and that a model trained on personal data is not automatically anonymous. They recommend data protection impact assessments for high-risk AI projects, treating consent as a last resort after other legal bases, and responding to deletion requests even when removing data from a trained model is technically difficult.

In **Vietnam**, the draft Data Security Law was introduced to the National Assembly and would establish five data security risk levels and a mechanism for monitoring and responding to incidents. Cross-border transfers would require no procedures for Level 1 and 2 data, self-assessment for Level 3, and prior approval for Levels 4 and 5, whose processing systems would also need assessment before use without handing over source code or model weights. AI developers and deployers would have to control the origin and integrity of training data and allow human intervention in automated decision-making. Additionally, the Ministry of Public Security consulted on a National Standard on basic cybersecurity requirements for Internet of Things devices, which would ban shared default passwords, require privacy by default and disclosure of cross-border data flows, and require an option for higher-risk devices to store and process data only in Vietnam.

Americas

In **Argentina**, the National Securities Commission opened a consultation on draft amendments to the relevant facts disclosure regime, which would require issuers and authorized market agents to immediately report operational, technological, and cybersecurity incidents that significantly hinder their activities.

In **Brazil**, the National Data Protection Agency adopted guidance on the scope and general obligations of the Digital Statute of Children and Adolescents for suppliers of information technology products and services. It clarifies the concept of "likely access" by children, under which the Statute as a rule applies to social networks, app stores, and operating systems, and sets out obligations such as protective default privacy settings, age assurance, parental supervision tools, and age signals from operating systems and app stores.

In **Canada**, the Office of the Privacy Commissioner (OPC) issued the Children's Privacy Code, guidance on how existing federal privacy law applies to online services directed at or likely to be accessed by people under 18. The Code says organizations should obtain parental consent for children under 13 and opt-in consent for non-essential uses, conduct privacy impact assessments, and not profile children for marketing or AI-based decisions. The Canadian Securities Administrators also opened a consultation on the proposed Regulation 26-101 on Information Technology System Integrity, which would consolidate IT obligations for marketplaces, clearing agencies, and other market infrastructures.

Regarding enforcement, Loblaw signed a compliance letter with the OPC after a data breach affecting about two million customers, committing to notify all affected individuals and to provide an independent external security assessment. The OPC also opened an investigation into Navigate360, which operates the tip platform used by Crime Stoppers programs across Canada, after a cybersecurity incident.

Africa

In **Kenya**, the Ministry of Information, Communications and the Digital Economy published the Access to Information Policy, 2026, which sets out how public and certain private bodies are to implement the right of access to information, including through digitized records and open data formats.

Digital Policy Alert

Contact
Written by Maria Buza and Sherif Taha
Please send questions and suggestions to maria.buza@sgept.org

The independent Digital Policy Alert is a pillar of the Swiss-based
St. Gallen Endowment for Prosperity Through Trade

St.Gallen Endowment
for Prosperity through Trade