



Digital Policy Alert

GLOBAL DIGITAL POLICY ROUNDUP

JULY 2026



Global Digital Policy Roundup: July 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 the [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](#) further allow you to navigate, compare, and chat with the legal text of AI rules across the globe.

Drawing from Digital Policy Alert's daily monitoring of developments in the G20 countries, it summarizes the highlights of July 2026 in four core areas of digital policy.

- **Content moderation**, including the European Commission's €550 million fine on AliExpress and preliminary findings against Meta and TikTok over compliance with minor protection obligations under the Digital Services Act, France's adoption of a bill restricting minors' access to social network services, Brazil's entry into force of decrees on content moderation and gender-based online violence, and the Republic of Korea's Act expanding the categories of prohibited illegal content under the Network Act.
- **AI regulation**, including the entry into force of the European Union's Digital Omnibus on AI Regulation, the signature of an agreement establishing the World Artificial Intelligence Cooperation Organization by 29 countries, Russia's Federal Law on Supporting the Development of AI Technologies, China's interim measures for the administration of anthropomorphic AI interaction services, and the introduction of five bills amending the Republic of Korea's AI Basic Act.
- **Competition policy**, including the European Commission's €460 million and €430 million fines on Alphabet under the Digital Markets Act, the General Court's dismissal of Apple's challenge to its gatekeeper designation, China's ¥5.18 billion fine on Trip.com for abuse of dominance, and the Republic of Korea's Fair Trade Commission's investigation into Google's Games Velocity Program.
- **Data governance**, including the European Data Protection Board's draft guidelines on web scraping to train generative AI models and on anonymization, the United Kingdom's Upper Tribunal decision upholding the Information Commissioner's Office's £12.7 million fine against TikTok, and the Republic of Korea's Personal Information Protection Commission's fines on Apple and TikTok over unlawful data collection and transfers.

Content moderation

Europe

In the **European Union**, the regulation extending the derogation from certain provisions of the ePrivacy Directive entered into force, allowing electronic communications services to continue the voluntary detection, removal, and reporting of online child sexual abuse material until April 2028.

The special panel on child online safety convened by the President of the European Commission presented its final report. It recommends an EU-wide framework that includes a minimum social media access age of 13, privacy-preserving age assurance, and harmonized safety-by-design requirements for digital services, among others. The Commission will now assess the recommendations and consider follow-up legislative proposals.

The Commission also continued enforcement of the Digital Services Act (DSA). It fined AliExpress €550 million for failing to mitigate risks related to illegal, unsafe, and counterfeit products. The Commission also issued preliminary findings that Meta failed to adequately assess and mitigate the addictive risks of Instagram and Facebook features, while TikTok's default account settings for minors exposed minors' content and profiles more broadly than required. If the Commission ultimately finds the companies non-compliant, it may impose fines of up to 6% of their global annual turnover. In addition, the Commission accepted X's action plan to address breaches relating to advertising transparency and researcher access, subject to implementation, an independent audit, and enhanced supervision.

At the **judicial level**, the Court of Justice of the European Union ruled that hosting gambling advertising on YouTube falls within the scope of the e-Commerce Directive, but found that Google may not benefit from the hosting liability exemption where it plays an active role in reviewing and partnering with content creators. The Court also ruled on the scope of the "operator" concept under Council Regulation imposing sanctions against Russia and held that streaming subscriptions constitute digital services rather than digital content under the Consumer Rights Directive.

At the **member state level**, Austria launched a consultation on a draft bill requiring certain video-sharing platforms to block access for users under 14 where adequate child protection measures are not in place. In Bulgaria, a bill was introduced that would prohibit children under 16 from creating or managing public or partially public social media and video-sharing platform profiles, without an exception for parental consent.

France's Parliament adopted the bill on protecting minors from the risks arising from the use of social networks, which had received a European Commission opinion earlier in the month. The bill prohibits access to online social network services for minors under 15, subject to limited exceptions, with implementation scheduled to begin in September 2026 following Constitutional Council review.

Regarding **enforcement**, France's Competition Authority imposed interim measures requiring Meta to resume good-faith negotiations with French press publishers over remuneration for the use of press content and to disclose information supporting its payment offers. The measures will remain in force pending the Authority's investigation into a possible abuse of dominant position.

Additionally, the French Regulatory Authority for Audiovisual and Digital Communication (Arcom) published an [analysis of advertising repository effectiveness](#) under the DSA, and extended the validity of Amazon Prime Video's amended service agreement until December 2026, allowing negotiations with the French film industry to continue. The agreement requires Amazon Prime Video to maintain its commitments to invest at least €90 million in European and French-language original content. Finally, Arcom opened an investigation into additional [pornographic sites](#) over non-compliance with age verification obligations.

The **German** Commission on Licensing and Supervision (ZAK) adopted a legal position stating that German media law applies to [Google's AI Overviews](#) and [Perplexity's AI chatbot and news feature](#). According to ZAK, AI-generated responses constitute the providers' own content rather than content covered by the Digital Services Act's liability exemption. It also considers AI search functionalities and chatbots that select and prominently display links or sources to qualify as media intermediaries, making them subject to obligations aimed at safeguarding media plurality and transparency. Furthermore, the 42nd Civil Chamber of the Munich Regional Court largely upheld [GEMA's claims against Suno](#), finding that the AI music generator unlawfully reproduced copyrighted musical works during model training and generated outputs that infringed copyright. The court held that these acts were not covered by Germany's text and data mining exception or by the US fair use doctrine and found Suno, rather than its users, responsible for the infringements.

The **Italian** Communications Regulatory Authority (AGCOM) consulted on [guidelines](#) on the integrity of online reviews. The proposed guidelines would require businesses to verify that reviews come from genuine consumers, increase transparency in review management, and prohibit misleading practices. AGCOM also ordered internet access providers to block access to an [Escort Advisor website](#) for failing to implement legally required age verification measures to protect minors. The blocking order will remain in force until the operator demonstrates compliance.

In **Turkey**, a law entered into force that expands the powers of the [Cyber Security Presidency](#) to regulate internet domain name policies and to order the rapid implementation of measures affecting internet content and access, requiring operators, access providers, and hosting providers to comply within 2 hours. The Law also introduces administrative fines for non-compliance and requires conditional access media service providers and internet platform operators to [contribute 2%](#) of their annual net sales to a fund supporting the Turkish film industry.

In the **United Kingdom**, the [Television Selection Services Regulations](#) entered into force, designating 15 services, including those from Amazon, Google, Roku, Samsung, Sky, LG, Apple, and Virgin Media, as regulated "television selection services" subject to prominence requirements for public service broadcasters. The Office of Communications (Ofcom) also issued the [Listed Events \(Coverage\) Regulations](#), extending the UK's listed-events regime to on-demand platforms and internet streaming services and setting rules for what counts as "live" and "adequate" coverage of protected sporting events.

Under the Online Safety Act, Ofcom adopted a [register of categorized services](#) subject to additional duties, and opened consultations on draft codes and guidance. The draft Fraudulent Advertising Code of Practice for [Category 1 services](#) applies to designated services including Facebook, Instagram, Pinterest, Quora, Reddit, Roblox, Snapchat, TikTok, WhatsApp, X, and YouTube. The draft code would require providers to implement risk-based systems to detect, review, and remove fraudulent advertisements, supported by user reporting and appeals

mechanisms. It would also require providers to maintain a searchable public advertising library, increase transparency regarding advertising moderation practices and automated detection technologies, and implement measures relating to testing, account checks, procedural safeguards, and governance and accountability. In parallel, Ofcom consulted on a corresponding Fraudulent Advertising Code of Practice for Category 2A services, including Google Search, Bing, ChatGPT Search, and Facebook Feed Deep Dive, proposing comparable requirements on content moderation, testing, account integrity, and account appeals measures.

In addition, Ofcom consulted on a draft Additional Duties Code of Practice for Category 1 services, covering user empowerment measures, complaints procedures, and the treatment of content of democratic importance and journalistic content. To support implementation of these obligations, Ofcom also published draft guidance addressing fraudulent advertising judgments, freedom of expression and privacy impact assessment, terms of service, journalistic content factors, news publisher content, user empowerment assessment, user identity verification, relevant content, and record-keeping and review.

Furthermore, Ofcom published its assessment of the use of age assurance, and the government announced age restrictions and online safety requirements for children under the Children's Wellbeing and Schools Act.

Regarding **enforcement**, Ofcom fined the provider of Fapello £630,000 for failing to comply with age assurance obligations, opened an investigation into TikTok's compliance with child protection and age assurance obligations, and issued a revised provisional notice of contravention to the provider of Im.ge over illegal content risk assessment duties. Ofcom also issued a provisional decision that the provider of an online suicide discussion forum breached the Act by failing to conduct adequate risk assessments.

Asia and Australia

Australia's House of Representatives passed the Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill, including provisions on increasing penalties for social media platforms that fail to enforce a minimum age requirement for users under 16. The Interactive Gambling Amendment (Gambling Reform) Bill was also introduced to the House of Representatives, including content moderation authority governance, content moderation regulation, fair marketing and advertising practices, and an age verification requirement. Additionally, the government announced laws to reduce the threshold for minors' claims against digital platforms and empower the Civil and Administrative Tribunal to issue demasking orders which would require social media companies to disclose the identities of anonymous users accused of online vilification.

Regarding **enforcement**, the Federal Court fined JustAnswer AU\$10 million over misleading and deceptive conduct in its online advice service. The eSafety Commissioner filed a lawsuit against Telegram over its alleged failure to remove pro-terror material and implement detection systems and separately published a report on measures against child sexual exploitation and abuse identifying safety gaps in how large technology platforms detect child sexual exploitation and sexual extortion.

China's State Administration for Market Regulation and Ministry of Commerce opened a consultation on amendments to the E-commerce Law. It includes measures to increase penalties

for platform non-compliance, expand government supervisory powers, and establish a tiered regulatory model for e-commerce platforms based on their scale and impact. CAC additionally opened a consultation on the Anti-Cyber Violence Law. It would define cyberbullying and establish obligations for platforms to detect, remove, and restrict the dissemination of harmful content, including through content removal, account measures, and rumor-refutation mechanisms. The Law further includes measures on [authority governance](#), [user rights](#), and [user identification](#).

Regarding **enforcement**, the CAC announced that, following its investigation into [AI applications](#) operated by Huawei, Alibaba, Zhipu, Xiyu, and DeepSeek, more than 6 million pieces of illegal or irregular information were removed, action was taken against over 26,000 accounts, and more than 1,300 AI products and nine illegal open-source datasets were taken down. Additionally, CAC confirmed enforcement action against [short video platforms](#) over improper content labeling and launched a [campaign](#) to address harmful online content and practices affecting minors, including AI-generated violent content, recruitment for intimate images, and predatory marketing tactics.

In **India**, a public interest litigation seeking restrictions on minors' access to [Roblox and other online gaming platforms](#) was filed against the Union of India. The Lok Sabha Standing Committee on Consumer Affairs, Food and Public Distribution issued a [report](#) recommending establishing a coordinated monitoring mechanism across multiple agencies to address mislabeling and misleading food listings on e-commerce platforms.

Regarding **enforcement**, the Food Safety and Standards Authority opened an investigation into [Swiggy Instamart](#) over alleged food safety violations, and the Central Consumer Protection Authority opened an investigation into [SpiceJet](#) over dark patterns, including pre-ticked checkboxes to auto-enroll users in loyalty and communications programs without explicit consent.

Indonesia's Ministry of Communication and Digital Affairs announced verification of [child protection requirements](#) across 14 digital services owned by Apple.

Japan's Ministry of Internal Affairs and Communications consulted on its report addressing [issues in information distribution in the digital space](#), including recommending mandatory age verification, risk assessments, and default protective measures for minors on digital platforms.

In the **Republic of Korea**, the Act on Promotion of Information and Communications Network Utilization entered into force. The Act expands the categories of prohibited illegal content to include discriminatory and harmful false or manipulated information and requires large-scale service providers to establish policies to identify and address such content. It also introduces punitive damages of up to five times the actual damages for the intentional or negligent distribution of harmful false information and establishes measures on [governance and oversight bodies](#), and [user objection rights](#). The Amended Enforcement Decree of the Network Act also took effect, covering [authority governance](#) and [content moderation measures](#). Amendments to the Enforcement Decree of the Act on Consumer Protection in E-Commerce entered into force, addressing [consumer review disclosure](#), [user identification](#), and [surcharge standards](#) for violations, while a related Partial Amendment to the Act advanced [consumer protection governance](#), [fair marketing practices](#), and [identity verification obligations](#). Separately, bills were introduced addressing the [suspension of music track distribution harmful to youth](#) and the [repeal of false and manipulated information and hate speech provisions](#) under the Network Act.

Americas

In **Brazil**, two decrees related to online safety entered into force. [Decree 12,975](#) updates content moderation rules to require removal of illegal third-party content upon notification, while requiring a court order for crimes against honor and for restricted communications services. It introduces systemic failure liability for categories including terrorism, incitement to suicide or self-harm, incitement to discrimination, gender-based violence against women, sexual crimes against vulnerable persons, and human trafficking. [Decree 12,976](#) establishes protections for women online and addresses gender-based violence in digital environments. It introduces content moderation duties for internet application providers hosting third-party content, requiring the removal of material linked to gender-based offenses or unlawful acts against women, including aggravated threats, stalking, psychological violence, and non-consensual dissemination of intimate content. Additional obligations include restrictions on the use of AI or similar technologies to generate or alter intimate content and requirements to detect and block such activity. Regarding enforcement, the National Secretariat for Digital Rights published a [report](#) identifying 32 websites offering artificial intelligence tools to generate synthetic nude images and assessing their availability and operating practices in Brazil. The report referred to law enforcement and the National Data Protection Agency for the assessment of potential legal violations and possible enforcement action.

Artificial Intelligence

International

Twenty-nine countries, including Brazil, China, Indonesia, Russia, and South Africa, signed an agreement establishing the [World Artificial Intelligence Cooperation Organization](#). The Asia-Pacific Economic Cooperation member economies issued a [statement](#) promoting AI development in the Asia-Pacific region. Fourteen countries, including Australia, Canada, France, Germany, India, Italy, Japan, the Republic of Korea, and Poland, adopted [guidance](#) on minimum elements for software bills of materials. Australia, Canada, and India also signed a Technology and Innovation Partnership.

Europe

The **European Union's** Digital Omnibus on AI Regulation entered into force. The Regulation clarifies the [AI Office's competences](#) for supervising AI systems based on general-purpose AI models, extends its enforcement powers to AI systems embedded in very large online platforms and search engines, expands access to [AI regulatory sandboxes](#), including an EU-level sandbox, and extends SME exemptions to small mid-cap enterprises. The Regulation also amends the AI Act's [design, quality of service, and cybersecurity](#) requirements for high-risk AI systems, the [legal basis for processing special categories of personal data for bias detection](#), and the [registration requirements](#) for high-risk systems. Furthermore, the Omnibus further amended the AI Act to prohibit, from December 2026, [AI systems](#) designed to generate child sexual abuse material or non-consensual intimate content of identifiable persons without adequate technical safeguards.

The European Commission published [guidelines](#) on the transparency obligations under Article 50 of the AI Act, clarifying disclosure requirements for AI systems that interact with users, generate synthetic content, or perform emotion recognition and biometric categorization. The guidelines

also explain compliance measures, applicable exemptions, enforcement penalties, and transitional timelines for certain generative AI systems. Additionally, the **Commission** adopted an [action plan on cybersecurity](#) and AI, and the European Committee for Standardization and the European Committee for Electrotechnical Standardization adopted a [quality management system standard](#) for AI Act regulatory purposes.

The **French** Competition Authority published a [report](#) on competition in the AI agents sector, identifying barriers to expansion and competition risks associated with vertically integrated providers and AI-enabled intermediary services. The report recommends regulatory oversight, improved interoperability and data portability, the development of technical standards, and closer monitoring of acquisitions and AI distribution channels. Additionally, the National Commission for Information Technology and Civil Liberties, together with the Council for AI and Digital Technology, published a [note](#) on the risks of agentic AI for personal data protection.

The President of **Russia** signed the [Federal Law on Supporting the Development of AI Technologies](#). The Law establishes a legal framework for the development, deployment, and use of large foundation AI models, provides for government support measures, defines requirements for [sovereign and national AI models](#), and introduces obligations relating to AI-generated content labeling and [intellectual property](#). It will enter into force in phases beginning September 2026.

In the **United Kingdom**, the Department for Business and Trade opened a consultation on the [use of workplace monitoring technologies](#), including AI-enabled monitoring and automated decision-making. The consultation seeks views on potential measures to improve transparency, worker engagement and accountability, including a statutory code of practice, consultation requirements for employers, or non-statutory guidance.

Asia and Australia

The government of **Australia** announced legislation on [standards for Artificial Intelligence](#), focused on environmental and energy requirements for large data centers, including obligations to pay for grid connections and contribute net energy to the power grid, and additionally to create an [Office of Artificial Intelligence](#). Moreover, the Cyber Security Centre published [guidance](#) on AI model harnesses for cybersecurity, finding that well-designed harnesses around mid-tier AI models can achieve comparable defensive capabilities to frontier models.

In **China**, the [interim measures](#) for the administration of anthropomorphic AI interaction services entered into force. The measures [prohibit](#) anthropomorphic AI services from manipulating users through emotional dependence, addiction, self-harm content, or replacing real social interaction. It prohibits providing virtual relative or virtual partner services to minors and requires providers to identify underage users, enable “minor mode,” obtain parental consent for users under 14, and provide appeal mechanisms. The measures set additional obligations on [design requirements](#), [data protection](#), [cybersecurity](#), [performance monitoring](#), [user rights](#), and [user identification](#). Furthermore, CAC issued [filing information](#) for 7 generative AI services integrated into mobile devices from Apple, Huawei, OPPO, Vivo, Xiaomi, Samsung, and Nubia and published the [eighteenth batch of deep synthesis service algorithms](#), registering algorithms for text generation, image synthesis, video creation, and audio generation services. CAC also opened consultations on a [national standard](#) for security classification in cybersecurity and AI applications, [AI browser security practice guidelines](#), and a [network security standard practice guide on AI agent interaction security](#).

In **India**, Delhi High Court dismissed ANI Media's copyright infringement lawsuit against [OpenAI](#), ruling that using published content to train AI models constitutes protected research under Indian copyright law.

In **Indonesia**, the Ministry of Communication and Digital Affairs announced the completion of the drafting of a [Presidential Regulation](#) to govern the use of AI. The Ministry also closed consultations on [annual reporting formats](#) for AI businesses to disclose business activities, technologies, infrastructure, and governance measures for regulatory supervision, and on a [corresponding format for the blockchain services sector](#) covering operational status, product offerings, and infrastructure for regulatory supervision.

In the **Republic of Korea**, five bills amending the AI Basic Act and related legislation were introduced to the National Assembly, addressing [non-discrimination requirements](#), [expanding the definition of high-impact AI affecting workers](#), [intellectual property governance](#), [generative AI disclosure requirements](#), and a [personal information use exception for AI development](#). The Ministry of Science and ICT also published an [AI security redteaming guide](#) and an [AI security threat response manual](#).

Saudi Arabia adopted a [National Framework for AI Risk Management](#) requiring government and private entities to classify and manage AI risks across areas including bias, privacy, security, and misinformation.

Competition

Europe

The **European** Commission fined Alphabet €460 million for [self-preferencing on Google Search](#) and €430 million for [restricting app developers' steering practices](#) on Google Play, both in breach of the Digital Markets Act (DMA). Additionally, the Commission adopted a final decision under the DMA requiring Google to [share search data](#) with competitors and opened a specification proceeding to support Google's compliance with [interoperability obligations](#) under the DMA. The Commission also opened an investigation into [Temu](#) over alleged distortive foreign subsidies granted by China, approved the [acquisition of Warner Bros. Discovery by Paramount Skydance](#), and accepted binding commitments from SAP closing an investigation into [enterprise resource planning software practices](#).

The General Court dismissed Apple's challenge to its [gatekeeper designation](#) under the DMA, and the Court of Justice dismissed Google's appeal of the [€4.125 billion fine](#) imposed over abuse of dominance related to the Android operating system.

In **Italy**, the Competition Authority fined [Lime Technology](#) €1.4 million for an unfair commercial practice involving barriers that prevented users from activating the Lime Transit Pass, a free-ride package linked to Rome's public transport subscription, and Bird Rides €750,000 for two unfair commercial practices related to its electric scooter sharing service. Additionally, the Authority opened a consultation on contract terms used by [Perplexity AI](#).

In the **United Kingdom**, the Competition and Markets Authority (CMA) consulted on proposed conduct requirements following the strategic market status designations of [Apple's](#) and [Google's](#) mobile platforms, and closed a call for evidence on [near-field communication access conditions](#) on Apple's platform. Furthermore, the CMA approved eBay's acquisition of [Depop](#), and Getty Images and Shutterstock terminated their proposed [merger agreement](#), formally notifying the CMA.

Asia and Australia

Australia's Competition and Consumer Commission opened a consultation on its determination regarding the [Google and Epic Games application store settlement agreement](#) capping Google Play service fees at 10 to 20% and permitting alternative payment options.

The State Administration for Market Regulation of **China** fined [Trip.com](#) ¥5.18 billion for abuse of dominance in online hotel reservations.

The Competition Commission of **India** dismissed a complaint against [Zomato](#) over alleged anti-competitive pricing practices, fined [HP India](#) ₹128.09 crore over bid manipulation, and approved upGrad Education's acquisition of [Sorting Hat Technologies](#).

The Business Competition Supervisory Commission **Indonesia** announced an investigation into [TikTok](#) over alleged abuse of market dominance, and released a one-year impact assessment of its earlier case against [Shopee](#) and Shopee Express, finding that the e-commerce ecosystem gained Rp1,477 trillion in benefits, but that algorithmic dominance remained.

Japan's Fair Trade Commission opened a consultation on amended [guidelines for merger review](#) under the Antimonopoly Act to address platform markets, indirect network effects, and data foreclosure in digital sectors.

In the **Republic of Korea**, a bill was introduced to amend the Monopoly Regulation and Fair Trade Act, mandating [review and accountability procedures](#) for Fair Trade Commission dispositions overturned by courts, and another bill would impose [commission caps and cost disclosure requirements](#) on delivery platform operators.

Regarding **enforcement**, Korea's Fair Trade Commission fined eight [SolidWorks software resellers](#) ₩2.372 billion over a price-fixing and customer-allocation cartel, and approved Mirae Asset Consulting's acquisition of [Korbit](#). It further initiated deliberation proceedings against [Analog Devices](#) and [NXP](#) over alleged semiconductor distribution restrictions, and opened an investigation into [Google](#) over its Games Velocity Program, which offered financial incentives to game developers in exchange for exclusive or most-favored-nation treatment on the Play Store.

Africa

The Competition Commission of **South Africa** referred Audatex to the Competition Tribunal for prosecution over alleged [price discrimination in vehicle repair estimation software pricing](#).

Data governance

Europe

The **European** Commission published [guidance](#) to support the implementation of the Cyber Resilience Act, clarifying its scope, product coverage, substantial modifications, support periods, reporting obligations and risk assessment requirements. Additionally, it opened a consultation on a [cybersecurity certification scheme](#) for EU Managed Security Services and on [international data sovereignty challenges](#). Separately, the Commission completed its first review of the 2021 [adequacy decision](#) for the Republic of Korea, confirming that the country continues to ensure an adequate level of protection for EU personal data transfers.

The European Data Protection Board (EDPB) opened consultations on draft guidelines addressing the legal basis and safeguards for [web scraping to train generative AI models](#) and on draft [guidelines](#) on anonymization, which introduce a three-part test, no record isolation, no linkage, and no inference, for assessing whether data is truly anonymous. It also adopted a second version of its [guidelines](#) on processing personal data through blockchain technologies, recommending permissioned blockchains and off-chain storage where possible. At a high-level meeting in Dublin, the EDPB called on the European Commission to propose a [legal basis for cross-regulatory information sharing](#) between regulators in adjacent fields, and set out measures to strengthen cross-border GDPR enforcement amid a rise in complaints linked partly to AI. The EDPB also wrote to the Commission on the US Supreme Court's judgment in *Trump v Slaughter*, asking it to assess the [ruling's implications](#) for the adequacy decision underpinning the EU-US Data Privacy Framework. Separately, the EDPB and the Anti-Money Laundering Authority announced [joint guidelines](#) on information-sharing partnerships under Article 75 of the Anti-Money Laundering Regulation, with public consultation expected in the first half of 2027.

In **Germany**, the Data Protection Conference launched a consultation on the [Stuttgart Impulses for the Modernization of Data Protection](#), inviting stakeholders to provide feedback on 10 proposals for reforming data protection supervision. The proposals address potential changes to the governance, coordination and operational processes of data protection authorities, including legal provisions, expertise sharing, digital access points and review procedures.

The **Italian** Data Protection Authority opened an investigation into [TIM](#) over alleged unlawful telemarketing and data-subject rights violations, and continued its investigation into [Lusha Systems](#) over alleged unauthorized processing of contact data.

In **Turkey**, the Data Protection Authority issued a [decision on personal data processing of accident victims](#) and a [guidance](#) note on the use of third-party personal data for advertising and marketing.

In the **United Kingdom**, the HM Treasury designated four cloud service providers as [Critical Third Parties](#) under financial services rules. The Department for Science, Innovation and Technology opened inquiries into [international data transfers](#) and [data regulation in the age of AI and other data-intensive technologies](#). Additionally, the Upper Tribunal dismissed [TikTok's](#) appeal against a ruling that the Information Commissioner's Office had the power to impose a £12.7 million fine for data protection breaches, including the unlawful processing of children's data. The Tribunal confirmed that TikTok's processing activities do not fall within the Data Protection Act 2018's

special purposes exemption, and the case will return to the First-tier Tribunal for consideration of the remaining issues.

Asia and Australia

Australia's Signals Directorate published guidance on [secure adoption of agentic AI systems](#) in cyber defense, [post-quantum cryptography vendor readiness](#), and [privacy requirements for facial recognition technology](#). The Cyber Security Centre also closed a consultation on the evolution of its [Essential Eight cybersecurity framework](#), providing threat-informed mitigations for contemporary IT environments.

In **China**, several technical standards entered into force, including [security requirements for data transaction services](#), [network virtualization security](#), [wireless network access security](#), [network security test platform architecture](#), [framework for public key cryptography application technology in network security](#), [data interface security risk monitoring methods](#) and [cybersecurity product interconnectivity](#) on alarm information format entered into force, alongside [security requirements for connected cameras](#) and [related labeling rules](#), and [security guidelines for intelligent agents](#). The Cyberspace Administration also adopted [simplified personal information protection measures for small processors](#) handling fewer than 100,000 people, reducing compliance obligations proportional to processor size. Further, the National Information Security Standardization Technical Committee opened consultations on national standards covering [data provision and collaborative processing](#), [anonymous entity identification](#), [security classification for cybersecurity and AI applications](#), and the [SM9 cryptographic algorithm](#), and opened a consultation on a [network data security risk assessment guideline](#).

Regarding **enforcement**, the Ministry of Industry and Information Technology issued notices against [32 mobile application developers](#) over breaches of data privacy rules.

Indonesia advanced a [Presidential Regulation](#) establishing an independent Personal Data Protection Authority.

Japan's amended Act on Protection of Personal Information entered into force. The Act expands the [Personal Information Protection Commission's](#) enforcement powers, introducing a mandatory administrative surcharge equal to the financial benefit gained from unlawful data handling affecting 1,000 or more individuals, with penalties rising for repeat violations, and increased criminal penalties for intentional data theft or unauthorized access. It also introduces new [categories](#) of "contactable personal-related information" and "specific biometric personal information," requiring advance notice and granting individuals rights to request suspension or cessation of use, with these rights exercised by legal representatives for individuals under 16.

In the **Republic of Korea**, the Personal Information Protection Commission (PIPC) opened consultations on a cluster of measures implementing amendments to the Personal Information Protection Act, including [investigation and disposition regulations](#), [complaint-filing standards](#), [disciplinary recommendation standards](#), [public announcement guidelines](#), and [administrative fine standards](#). Additionally, several bills were introduced to strengthen [notification obligations and security measures for unauthorized access](#), to increase [penalties for illegal distribution of leaked personal information](#), to reduce fines for [operators running vulnerability reward programs](#), to strengthen [data preservation obligations for security incident analysis](#), and to introduce a [personal information use exception for AI development](#).

Regarding **enforcement**, the PIPC fined Apple ₩252 million and TikTok ₩10.3 billion over unlawful data collection and transfers. Additionally, the PIPC fined Korea Telecom ₩539.8 billion over personal information leakage through unauthorized femtocells and referred LG Uplus to law enforcement over alleged personal data breaches.

Americas

In **Argentina**, a bill was introduced to the Chamber of Deputies establishing a new Personal Data Protection Law, covering cross-border data transfer, data protection authority governance, and general data protection regulation.

In **Brazil**, the National Data Protection Authority concluded its monitoring of data protection officer appointment obligations and considered sanctions, and renewed a Technical Cooperation Agreement with the Competition Authority.

Canada's Securities Administrators published a review of registered firms' cybersecurity practices, and the Office of the Privacy Commissioner released guidance for reporting entities on codes of practice under anti-money laundering legislation.



Contact
Written by Maria Buza and Aishwarya Vaithyanathan
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

