



GLOBAL DIGITAL POLICY ROUNDUP

APRIL 2026



Global Digital Policy Roundup: April 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 the Digital Policy Alert's daily monitoring of developments in the G20 countries, it summarizes the highlights of April 2026 in four core areas of digital policy.

- **Content moderation**, including the United Kingdom's Crime and Policing Act criminalizing nudification tools and AI-generated child sexual abuse material, Turkey's law prohibiting social network providers from offering services to children under 15, and the European Commission's preliminary findings against Meta under the Digital Services Act for failing to prevent minors from accessing Facebook and Instagram.
- **AI regulation**, including China's adoption of interim measures on anthropomorphic AI interaction services prohibiting emotional manipulation and restricting minors' access, Saudi Arabia's draft responsible AI policy, and Mexico's General Law to Regulate and Promote the Use of AI.
- **Competition policy**, including the European Commission's preliminary findings against Google under the Digital Markets Act for non-compliance with search data sharing obligations, its supplementary statement of objections to Meta over third-party AI assistants' access to WhatsApp, the UK Competition and Markets Authority's acceptance of final commitments from Google and Apple on app distribution and iOS interoperability, and China's prohibition of Meta's acquisition of the Manus.
- **Data governance**, including France's decree on sensitive data protection in cloud services, the Irish Data Protection Commission's investigation into Shein over the transfer of personal data to China, the Italian Data Protection Authority's EUR 12.5 million fine against Poste Italiane and PostePay, and Argentina's data protection bill.

Content moderation

International

The Council of Europe's Committee of Ministers adopted a [recommendation](#) on online safety and empowerment of users and content creators. It calls on Member States to establish legal frameworks on online safety, platform accountability, and user empowerment, while ensuring that content restrictions remain lawful and proportionate. The recommendation also encourages platforms to adopt safety-by-design measures, conduct risk assessments, and enhance user transparency and control over content moderation and recommendation systems.

Europe

The **European** Parliament adopted a [resolution on cyberbullying and online harassment](#) outlining recommendations for platform accountability and coordinated legislative responses to online violence. The European Commission adopted a [recommendation](#) establishing a common EU approach to age verification technologies, promoting privacy-preserving, anonymous proof-of-age methods. It calls on Member States to make such solutions available by the end of 2026 and introduces a coordination framework to support implementation.

Regarding enforcement, the European Commission preliminarily found [Meta](#) in breach of the Digital Services Act (DSA) for failing to effectively prevent children under 13 from accessing Instagram and Facebook. Meta's existing measures were deemed inadequate both to block underage access and to identify and remove minors who have already gained access to its services. The Commission also published hate speech compliance assessments of [X](#), [Viber](#), [Twitch](#), [Meta](#), [YouTube](#), and [TikTok](#) under the code of conduct on countering illegal hate speech online integrated into DSA. At the member-state level, Portugal implemented the [Law](#) designating competent national authorities and the coordinator under the DSA.

Italy's Communications Regulatory Authority filed a request with the European Commission to evaluate [Google's AI services](#) over alleged systemic risks to publishers and AI-generated misinformation. The Authority indicated that the request could lead to an investigation into potential breaches of obligations applicable to very large search engines, particularly regarding systemic risk mitigation measures related to freedom of information, media pluralism, and the transparency of recommendation systems.

In **Germany**, the Federal Ministry of Justice and Consumer Protection opened a consultation on a draft [bill](#) addressing digital offences such as hate speech, non-consensual intimate imagery, cyberstalking, harassment, and deepfakes, with provisions for criminal prosecution and civil remedies for violations of personality rights. It also requires platforms, in line with DSA obligations, to comply with judicial orders to remove unlawful content or suspend accounts.

The President of **Turkey** signed a [law](#) prohibiting social network providers from offering services to children under 15, effective November 2026. Users aged 15 and above can be granted access only to differentiated services with appropriate protections for minors. The law also introduces content moderation obligations for social network providers, grants [expanded powers](#) to the Information and Communication Technologies Authority, and requires foreign-based game platforms with daily access exceeding 100,000 to designate a [legal representative](#).

In the **United Kingdom**, two Acts received royal assent. The Crime and Policing Act criminalises the making, adapting, supplying, or offering of specific products and services, including “nudification tools”, AI models designed or optimised to generate child sexual abuse material, and instructional material on producing such content using AI. Further, the Act requires online platforms to remove non-consensual intimate images within 48 hours of notification. The Children's Wellbeing and Schools Act empowers the Secretary of State to issue regulations to restrict children's access to specified internet services or their functionalities, following the conclusion of the inquiry into the matter.

Regarding **enforcement**, the Office of Communication (Ofcom) published a confirmation decision against 4chan, imposing penalties totaling GBP 520,000 for failure to comply with illegal content risk assessment, illegal content safety, and children's safety duties. Ofcom also opened investigations into the messaging service providers Telegram, Chat-Avenue, and Teen-Chat, for allegedly failing to prevent users from encountering child sexual abuse material and to adequately reduce the risk of their services being used to share such content. Finally, Ofcom also closed its investigation into Yolobit after the service became unavailable in the country.

Asia and Australia

The **Australian** Treasury opened consultations on three bills covering administration, charges, and tax non-deductibility, establishing a news bargaining incentive framework intended to facilitate compensation from digital platforms to Australian news publishers for the use of their content. Additionally, the government responded to the statutory review of the Online Safety Act, committing to introducing a risk-based digital duty of care for online service providers. The eSafety Commissioner published guidance on assessing the application of online safety codes and standards under the Online Safety Act, supporting electronic service providers in identifying which obligations apply to their services in relation to unlawful and age-restricted material.

Regarding **enforcement**, the eSafety Commissioner issued transparency reporting notices to Roblox, Minecraft, Fortnite, and Steam over alleged facilitation of child grooming and radicalization on their platforms. The Minister of Communications confirmed Roblox's commitment to strengthening safety protections for users under 16, following the regulatory intervention in February 2026. Finally, the eSafety Commissioner and the Office of the Information Commissioner signed a memorandum to coordinate the implementation of age assurance requirements.

China's State Administration for Market Regulation issued a notice on the governance of the internet advertising ecosystem. It requires platforms to regulate advertising ranking systems and bans certain categories of advertising content, including the use of AI to impersonate individuals and content affecting minors. It also issued a notice on enforcement priorities for rectifying the internet advertising market order. Regarding enforcement, the Cyberspace Administration concluded its investigation into CapCut, Jianying, Maoxiang, and Jimeng AI for non-compliance with rules on labelling AI-generated content and directed local authorities to take administrative action and impose penalties.

India's Ministry of Electronics and Information Technology (MeitY) adopted the implementing rules on the law banning online money games. The rules classify online games into social games and e-sports, and prohibit online money games involving stakes or monetary rewards. The rules also establish the Online Gaming Authority to determine game categories, register e-sports, regulate

financial transactions, set safety and data rules, and coordinate enforcement. Operators must register or be classified, display status, follow grievance and compliance systems. The MeitY also extended the consultation [amendments](#) to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. The amendments clarify that existing requirements for preserving removed content and retaining user registration data for 180 days apply without prejudice to longer or stricter retention obligations under other applicable laws. Additionally, the MeitY issued an [advisory](#) requiring VPN providers and intermediaries to comply with IT Act due diligence obligations and online gaming restrictions, including blocking access to unlawful gambling platforms.

Indonesia's Ministry of Communication and Digital Affairs confirmed that [X](#), [Meta](#), [YouTube](#), [Roblox](#), and [TikTok](#) have introduced age verification systems and deactivated minors' accounts in compliance with child protection regulations.

In **South Korea**, a [bill](#) was introduced to the National Assembly to establish safety requirements for products intended for children aged 13 or younger. It requires manufacturers to ensure compliance through certification, self-regulation, or supplier inspections, and extends obligations to manufacturers, distributors, and e-commerce intermediaries. Regarding enforcement, the Fair Trade Commission issued corrections to unfair contract terms across [seven platforms](#), including Coupang, Naver, and Gmarket, and separately issued corrections addressing [arbitrary operating rights and settlement disadvantages](#) in e-commerce platform agreements.

Artificial Intelligence

Europe

The **European** Commission closed consultations on the draft implementing regulation under the Act. It covers the [enforcement procedures](#) governing the conduct of proceedings against AI system providers and deployers, and provisions on [access to data](#) from general-purpose AI models under investigation. Additionally, the Commission announced the launch of a [digital dialogue](#) with Morocco, with AI regulation among the areas covered. At the member-state level, the Polish Personal Data Protection Office submitted its [opinion](#) on the draft Act that implements the EU AI Act into national law, welcoming changes that removed provisions affecting its competences, but noted that the rules on cooperation with the new AI Commission remain unclear. It also called for its role to be explicitly recognized in the Act. The Dutch Authority for Financial Markets adopted a [report on the use of AI in capital markets](#), examining adoption rates, use cases, and risk management practices among market participants.

The **Italian** Competition Authority closed its investigation into the AI assistant [Nova](#) after the company committed to improving user-facing disclosure about the risk of factual inaccuracies in AI-generated outputs.

Russia's Ministry of Digital Development closed the consultation on the [draft Law on Fundamentals of State Regulation of AI Technologies](#), and is currently preparing the final draft before the government approves it and submits it to the State Duma. The draft Law would impose obligations on AI developers to eliminate features capable of producing discrimination based on behavioural or personal characteristics, to document model architecture, functional logic, and limitations, and to conduct risk modelling for technologies under development. It would also

restrict the use of AI in state information systems and critical information infrastructure owned by state bodies, institutions, and enterprises to designated "trusted" AI models, which would be required to process data exclusively within Russian territory. The draft law also includes measures regarding governance, design requirements, performance monitoring, testing obligations, user rights, and copyright protection measures.

In the **United Kingdom**, the Secretary of State issued regulations under the Data Protection Act requiring the Information Commissioner's Office to develop a code of practice on the use of personal data in AI and automated decision-making systems, including guidance on children's data. The regulations also exclude national security-related matters from the scope of the Act's panel reporting requirements.

Asia and Australia

Australia's Cyber Security Centre issued guidance on the cybersecurity implications of frontier AI models for organizations across all sectors, including critical infrastructure and government. It recommends reducing attack surfaces, applying regular patching, and strengthening systems through network segmentation and defense-in-depth. It also recommends the use of AI to detect and fix software vulnerabilities before deployment, aligned with existing security frameworks.

The Cyberspace Administration of **China** (CAC), together with four co-issuing regulatory authorities, adopted the interim measures for the administration of anthropomorphic AI interaction services. 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. Separately, the National Information Security Standardisation Technical Committee consulted on guidelines on ethical and security governance for AI applications and on cybersecurity guidelines for the deployment of OpenClaw-type agents, while the National Computer Network Emergency Response Technical Team issued an advisory on the secure deployment and use of OpenClaw AI agents. The Ministry of Industry and Information Technology closed a consultation on safety requirements for autonomous driving systems of intelligent and connected vehicles. At the **judicial level**, the Hangzhou Intermediate People's Court issued a judgment determining that companies may not terminate employment contracts solely for the purpose of replacing workers with AI systems. The Court found that AI adoption is not a "major change in objective circumstances" under Labour Contract Law and therefore does not justify termination. Employers must instead consider reasonable reassignment without significant pay cuts and cannot shift the costs of technological change onto employees.

India's Ministry of Electronics and Information Technology established the AI Governance and Economic Group to align government action on AI across sectors, including economic, security, and labour impacts.

In **South Korea**, the Personal Information Protection Commission held meetings to promote AI and robotics development through the use of pseudonymised data as part of a regional strategy. It addressed barriers to data use and strengthening institutional and technical support for safe

AI-driven growth. Additionally, South Korea and Indonesia signed a [memorandum](#) of cooperation on AI development and cybersecurity.

The **Saudi Arabia** Data and AI Authority opened a consultation on a [draft responsible AI policy](#) proposing organizational and governance requirements for entities developing and deploying AI systems.

Americas

Canada's Department of Innovation, Science, and Economic Development opened applications for the [AI Sovereign Compute Infrastructure Program](#), focused on building AI supercomputing infrastructure.

In **Mexico**, the Senate Commission for Analysis, Monitoring, and Evaluation on the Application and Development of AI announced its intention to submit a [General Law to Regulate and Promote the Use of AI](#). The proposal draws on six consultations, three technical papers, and elements from ten AI-related legislative initiatives. It addresses the potential impact of AI on small and medium-sized enterprises and sets out a framework aligned with international commitments on freedom of expression, while outlining a role for the government in supporting digital transformation.

Africa

The Department of Communications and Digital Technologies of **South Africa** withdrew the [draft national AI policy](#) from public consultation following an internal review that identified fictitious references in the document. The draft had proposed a risk-based governance framework for AI applicable across public and private sectors, with priority areas including healthcare, education, agriculture, and public administration. It also outlined the establishment of several institutions, including a National AI Commission, an AI Ethics Board, and a compensation mechanism for AI-related harm.

Competition

Europe

The **European Commission**, together with the European Parliament and the Council, jointly adopted the [One Europe, One Market Roadmap](#), a cross-institutional commitment to eliminate remaining barriers to the EU single market. It outlines legislative initiatives to be prioritized by the end of 2027, including the Digital Networks Act, Cloud and AI Development Act, European Business Wallet, and AI Gigafactories, among others.

The European Commission opened a consultation on the [draft merger guidelines](#). The draft expands the assessment criteria beyond price effects to include factors such as innovation, sustainability, resilience, privacy, and diversity, while addressing coordinated effects, algorithmic pricing, efficiencies, and Member State interventions on public security and other legitimate interests. The Commission also adopted the [Technology Transfer Block Exemption Regulation](#) and accompanying [guidelines](#) on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements.

The European Parliament adopted a [resolution](#) calling on the European Commission to fully enforce the Digital Markets Act (DMA), while expressing concerns that penalties against Meta and Apple were too limited relative to the alleged infringements. The resolution identified compliance concerns relating to Alphabet, Apple, ByteDance, Microsoft, and Booking practices and requested further assessment of AI-driven search and assistant services. The day before the resolutions' adoption, the European Commission published the [report](#) following its first review of the DMA, concluding that the framework remains fit for purpose and increased opportunities for businesses and developers while giving users greater choice, interoperability, and control over data and default digital services. It also noted that cloud services and AI are future focus areas.

Regarding **enforcement**, the European Commission issued preliminary findings to [Google](#) under the DMA proposing measures that would require the company to share search-related data with third-party search engines and AI search services on fair, reasonable, and non-discriminatory terms. The proposed measures address eligibility, scope, and frequency of data sharing, anonymization, pricing parameters, and access procedures. Additionally, the Commission opened a consultation on specification proceedings to support [Google's](#) compliance with Android interoperability requirements. The Commission also issued a supplementary statement of objections to [Meta](#), indicating its intention to require the restoration of third-party AI assistants' access to WhatsApp under equivalent conditions. At the **member-state level**, the Hungarian Competition Authority issued a ruling ordering [Temu](#) to pay HUF 1.3 billion for unfair commercial practices on its e-commerce platform.

The **Italian** Competition Authority opened an investigation into [Booking](#) over alleged unfair commercial practices linked to the presentation of accommodation under its partner preferred programmes. The Authority alleges that properties paying higher commissions receive preferential visibility and quality-related claims that may mislead consumers. Further, the Authority closed a consultation on its [sector inquiry into quantum computing](#).

The Competition Authority of **Turkey** launched a [sector inquiry into the AI ecosystem](#) to assess how AI development affects market dynamics and to identify emerging competition risks across infrastructure, model development, and applications. The inquiry will examine access to data, computing power, expertise, and funding, as well as AI-related mergers and acquisitions, to inform future policy and enforcement.

The **United Kingdom** Competition and Markets Authority (CMA) opened consultations on revised transparency and disclosure [guidance](#) under the Digital Markets, Competition and Consumer Act, and on [draft guidance](#) on the application of the Chapter I prohibition to technology transfer agreements. Regarding enforcement, the CMA accepted and published the final commitments of [Google](#) on app distribution and of [Apple](#) on app distribution and iOS interoperability, both arising from their respective strategic market status designations under the digital markets competition regime. The CMA published an interim report on remedies in its investigation into [Shutterstock's acquisition of Getty Images](#), and concluded consultations in its investigations into the anticipated acquisitions of [Depop by eBay](#) and [Warner Bros. Discovery by Paramount Skydance Corporation](#).

Asia and Australia

In **Australia**, a [bill](#) was introduced to the House of Representatives to prohibit unfair trading practices that manipulate consumer decision-making or distort choice where detriment is likely to

result. It also introduces transparency requirements regarding prices, including transaction-based charges, and sets new rules for subscription contracts and exit mechanisms. Additionally, the Competition and Consumer Commission (ACCC) opened a consultation on a determination proposing to deny [Screen Producers Australia](#) authorization to engage in collective bargaining with streaming services on model contract terms. Finally, the Federal Court granted the ACCC leave to intervene in [Epic Games v Apple](#) proceedings concerning relief arising from prior findings of misuse of market power by Apple in the app distribution market.

In **China**, the Office of the Foreign Investment Security Review Mechanism at the National Development and Reform Commission prohibited Meta Platforms' acquisition of the Manus project under the foreign investment security review framework.

In **South Korea**, the National Assembly adopted a [bill](#) expanding the composition of the Fair Trade Commission under amendments to the Monopoly Regulation and Fair Trade Act. The Fair Trade Commission also adopted and brought into force revised [standards for imposing surcharges](#) under competition law.

In **Brazil**, an [ordinance](#) establishing transparency rules for price composition and allocation on digital transport and delivery platforms entered into force. It requires platforms in the food delivery and ride-hailing sectors to disclose their pricing methodologies to users.

Africa

In **South Africa**, the [Electronic Communications Amendment Bill](#) was introduced to Parliament to set mandatory access obligations for large network operators. The bill also implements a "use it or share it" framework for spectrum, requiring unused licensed spectrum to be made available to secondary users after two years of non-utilisation. Furthermore, the Competition Commission opened a consultation on a [review of regulatory barriers to competition](#), examining their effects on small and medium enterprises.

Data governance

Europe

The **European** Data Protection Board (EDPB) adopted a [report](#) summarizing its regulatory activities and enforcement actions, and opened consultations on a [standardized template](#) for data protection impact assessments and on [guidelines](#) on the processing of personal data for scientific research purposes. The EDPB also adopted an [opinion](#) on the Europrivacy Certification Scheme Extension, addressing the use of the scheme as a transfer mechanism under Article 46 General Data Protection Regulation (GDPR) to certify data importers.

Regarding **enforcement** at the member-state level, the Irish Data Protection Commission (DPC) opened an inquiry into Infinite Styles Services (Shein) regarding the company's transfer of personal data of European Union and European Economic Area data subjects to China. Further, the Irish Supreme Court dismissed an appeal by the Data Protection Commission and continued the stay on suspension and compliance orders against [TikTok](#) arising from the Commission's investigation into alleged GDPR data transfer violations. Finally, the Amsterdam Court of Appeal ordered [X](#) to

disclose user data to a claimant and clarified users' access rights in the context of automated content moderation decisions under data protection law.

In **France**, the Prime Minister signed a decree on sensitive data protection in cloud services provided to state administrations, establishing localization and sovereignty requirements for public sector cloud procurement. At the judicial level, the Council of State issued a ruling in proceedings brought by La Quadrature du Net and others, partially annulling the government's refusal to repeal a decree on automated personal data processing for copyright protection on the internet, applying the Court of Justice of the European Union's judgment on national authority access to IP-address identification data.

Germany's Federal Office for Information Security published the criteria enabling cloud computing autonomy, a framework for assessing the technical and contractual conditions under which cloud service customers can maintain operational independence from their cloud providers. At the judicial level, the Stuttgart Higher Regional Court partially upheld a GDPR appeal against Meta Platforms, finding its processing of personal data via Meta Business Tools unlawful due to insufficient transparency about data use, storage, and security-related processing. The Court ordered full disclosure, restricted further processing pending compliance, and required deletion of unlawfully processed data after disclosure.

The **Italian** Data Protection Authority imposed fines totaling EUR 12.5 million against Poste Italiane and PostePay and ordered cessation of personal data processing through the BancoPosta and PostePay mobile applications. The Authority found that the companies had processed user data without a lawful basis.

In the **United Kingdom**, the Home Office issued the regulations updating the list of public authorities empowered to request access to communications data under the Investigatory Powers Act framework. Additionally, the Information Commissioner's Office published updated guidance on storage and access technologies under the Data (Use and Access) Act, addressing cookie and tracker compliance obligations.

Asia and Australia

Australia's Cyber Security Centre published guidance on security risks in social media and messaging services, assessing the data security practices and risk profiles of major platforms and providing recommendations for government and enterprise users.

The National Cybersecurity Standardisation Technical Committee of **China** closed the consultations on three national standards: the revised trusted computing specification for server trusted support platforms, cybersecurity technology methods for visual representation of cyberspace security, and a standard on capability requirements for personal information protection compliance audit institutions. Additionally, the Ministry of Commerce submitted formal comments to the European Commission, citing concerns about the proposed directive amending the NIS2 cybersecurity framework and its potential implications for Chinese technology companies providing digital services in the European Union.

In **South Korea**, a bill amending the Act on Promotion of Information and Communications Network Utilisation and Information Protection was introduced to the National Assembly. The bill would allow minors and their legal guardians to request the removal of content that may harm a

minor's privacy, reputation, or healthy development, and requires information and communication service providers to implement temporary measures immediately upon receiving a request. If no objection is raised within 30 days, the content must be permanently deleted.

Americas

In Argentina, a bill was introduced to the Chamber of Deputies to replace the existing data protection framework. The bill establishes principles-based obligations, including legality, purpose limitation, data minimisation, accuracy, limited retention, security, transparency, and proportionality. The bill also addresses deletion requests for data used in prior AI training by establishing technical viability assessments and requiring documentation of impossibility when deletion compromises model integrity, with alternative mitigation measures including blocking future use and exclusion from new training cycles. The bill further includes measures regarding enforcement and cross-border data transfer rules.

In **Brazil**, the National Data Protection Authority opened a consultation on guidance for suppliers of information technology products and services under the Digital Statute of Children and Adolescents, clarifying data protection obligations for technology providers whose products and services are used by children and adolescents.



Digital Policy Alert

Contact

Written by Tommaso Giardini and Maria Buza
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
