Digital Policy Alert

GLOBAL DIGITAL POLICY ROUNDUP

MAY 2026

Global Digital Policy Roundup: May 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

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 May 2026 in four core areas of digital policy.

- **Content moderation,** including the European Commission's EUR 200 million fine against Temu under the Digital Services Act, the entry into force of India's online gaming rules prohibiting online money games, and Brazil's decrees establishing online protections for women and addressing gender-based violence in digital environments.
- **AI regulation,** including the European Parliament and Council's provisional agreement on the Digital Omnibus on AI Regulation, China's implementation opinions on the standardized development of intelligent agents, and the Canadian privacy authorities' findings following the investigation into OpenAI.
- **Competition policy,** including the UK Competition and Markets Authority's strategic market status investigation into Microsoft's business software ecosystem, South Korea's Fair Trade Commission inquiry into the AI services market, and the Supreme Court of India setting aside the Competition Commission of India's order on Amazon's acquisition of a stake in Future Coupons.
- **Data governance,** including the Council of Europe's revised draft guidelines on data protection for large language model systems, the EUR 100 million fine against Yango by the Finnish, Dutch, and Norwegian data protection authorities, India High Court's ruling upholding the right to be forgotten and ordering global de-indexing of judicial records, and the Canadian Office of the Privacy Commissioner's guidelines on age assurance.

Content moderation

International

The **Group of Seven** Industry, Digital, and Technology Ministers adopted common principles for a safer and more secure digital space for minors. The principles call on digital service providers to implement safety-by-design measures, age assurance mechanisms for age-restricted services, and measures to prevent the generation and distribution of child sexual abuse material and non-consensual intimate images, including those generated using AI.

Europe

The **European Commission** opened a consultation as part of the review of the Directive on Copyright in the Digital Single Market, gathering evidence on possible policy measures relating to online piracy of live content, AI and copyright, protection against AI-generated impersonation of performers, and remuneration for recorded music. The Commission also ran a consultation as part of the review of the Audiovisual and Media Services Directive.

The European Commission continued the implementation of the Digital Services Act (DSA). It opened a consultation on the draft guidelines on the trusted flagger mechanism and released a related implementation study. The draft guidelines clarify the conditions for awarding, suspending, and revoking trusted flagger status, including requirements related to expertise, independence, and notice accuracy, as well as obligations for online platforms and transparency reporting.

Regarding **enforcement**, the Commission fined Temu EUR 200 million under the DSA for failing to adequately assess systemic risks related to illegal products on its platform. The Commission found that the platform's assessment relied on general sector-level data rather than platform-specific analysis. Temu must submit an action plan by the end of August 2026, which will be reviewed by the European Board for Digital Services and the Commission, with possible further measures in case of non-compliance. At the **member state level**, the **Irish Media Commission** opened investigations into Meta regarding compliance with DSA requirements on recommender system transparency and interface design.

At the **judicial level**, the **Court of Justice of the European Union** (CJEU) ruled on the compatibility of Italy's fair-remuneration framework with the Directive on copyright in the Digital Single Market. The CJEU held that EU law allows a system of fair remuneration for publishers, provided it remains linked to authorized uses and that publishers retain the choice to permit or refuse use free of charge. The CJEU also found that obligations on platforms to negotiate with publishers, share relevant data, and comply with national regulatory criteria, as well as related enforcement powers for regulators, are permissible. Separately, the CJEU held that Article 3 of the European Media Freedom Act does not apply ratione temporis to press rectification disputes predating 8 November 2024.

Finally, European Commission services responsible for the enforcement of the DSA signed a cooperation arrangement with Japan's Ministry of Internal Affairs and Communications on digital platform regulation to facilitate information exchange and coordinated supervisory approaches.

In **Germany**, the Federal Ministry of Justice and Consumer Protection consulted on the draft bill addressing digital offenses 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.

In the **United Kingdom**, the Office of Communications (Ofcom) provided advice to the Department for Science, Innovation, and Technology on the establishment of minimum standards of accuracy for accrediting detection technologies for terrorism and child sexual exploitation and abuse content. Ofcom also released guidance on technology notices on dealing with such content and a separate notice on extreme pornography duties specifying that realistic depictions of non-consensual sexual activity, including content depicting persons who are asleep or unconscious, are likely to constitute illegal content.

Ofcom opened a consultation on the draft standards code for designated video-on-demand services, covering protections for under-18s, harm and offense, crime and disorder, due impartiality and accuracy, elections and referendums, and fairness. It also released the draft accessibility code aimed at improving access for users with visual or hearing impairments.

Regarding intimate image abuse, Ofcom published the updated draft illegal content codes of practice for search services and user-to-user services. The proposed measures would require high-risk and large services to use hash-matching technologies to detect such content in images and videos, supported by human moderation, with applicability based on user reach and risk profile. The draft codes were submitted to the Secretary of State and are subject to parliamentary approval. Additionally, Ofcom issued a statement on additional detection measures and released draft guidance on the proportion of human review for hash matching.

Regarding **enforcement,** Ofcom imposed a GBP 950,000 penalty on the provider of an online suicide discussion forum for failures to comply with illegal content duties. It also fined Youngtek Solutions GBP 600,000 for failures relating to age assurance measures aimed at limiting minors' access to pornographic content, as well as for non-compliance with information request obligations. In addition, Ofcom opened investigations into Kemono and Pimpbunny and expanded its ongoing investigation into XGroovy, all concerning age assurance requirements for limiting access to pornographic content.

Ofcom also accepted X's commitments addressing illegal hate and terrorist content affecting UK users. X agreed to review UK-reported suspected illegal terrorist and hate content via its dedicated reporting tool within an average of 24 hours and to restrict UK access to accounts linked to proscribed organizations, where applicable. X also committed to engaging with expert organizations, providing quarterly performance data to Ofcom over 12 months, while Ofcom's investigation into X's compliance with its duties to address illegal content remains ongoing. Finally, Ofcom published reports on the child protection measures provided by Facebook, Instagram, Snapchat, Roblox, TikTok, and YouTube, covering measures relating to grooming risks, contact from unknown adults, and the role of recommender systems in surfacing content to children. In its assessment, Ofcom stated that the commitments set out may not prevent under-13s from accessing the platforms, and it noted that it was continuing to review the responses on recommender systems and content moderation.

Asia and Australia

The **Australian** Treasury consulted on three bills covering administration, charges, and tax non-deductibility that establish the news bargaining incentive framework intended to facilitate compensation from digital platforms to Australian news publishers for the use of their content. Separately, the Digital Platform Regulators Forum, comprising the Competition and Consumer Commission, the Communications and Media Authority, the eSafety Commissioner, and the Office of the Information Commissioner, issued a joint statement supporting the development of minimum internal dispute resolution standards for digital platforms.

Regarding **enforcement**, the Federal Court imposed a penalty of AUD 650,000 on X for failure to respond adequately to a February 2023 reporting notice from the eSafety Commissioner on its compliance with the Basic Online Safety Expectations regarding child sexual exploitation and abuse material. Additionally, the eSafety Commissioner issued a compliance direction to an Argentina-based AI "nudify" service requiring it to implement stronger age-verification measures within 14 days. The Commissioner noted that non-compliance could result in civil penalties of up to AUD 49.5 million and search engine delisting. In addition, the Competition and Consumer Commission commenced proceedings against Amazon over alleged breaches of safety standards for children's products sold by third-party sellers.

In **China**, the measures on the administration of internet public fundraising service platforms entered into force. The measures prohibit the insertion of commercial advertising into fundraising pages, the inclusion of links to commercial activities such as e-commerce or financial services, and the embedding of unrelated interactive features such as lotteries or promotional games. The framework also requires platforms to operate in line with principles of legality, good faith, voluntariness, fairness, and openness.

Separately, the Ministry of Public Security and other authorities issued regulations on internet information content distribution services, setting out obligations for platform providers, including social media and video-sharing services. It requires the establishment of complaint and reporting channels for multi-channel network operators, handling user complaints, and taking enforcement action against non-compliant operators, with suspected criminal cases to be referred to public security authorities. In addition, the Cyberspace Administration published guidance on online reporting, online rumor debunking, and online infringement reporting. The guidelines standardize reporting procedures across large platforms, including Tencent, Douyin, Weibo, Bilibili, Xiaohongshu, Kuaishou, Toutiao, and Baidu, and the central reporting system.

In **India,** the rules on the promotion and regulation of online gaming entered into force. 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, and follow grievance and compliance systems.

Regarding **enforcement**, the Central Consumer Protection Authority fined McAfee for deploying dark patterns in its subscription renewal interface. Additionally, the Ministry of Consumer Affairs directed the Authority to investigate online ticket booking platforms over alleged excessive cancellation charges, and the Directorate of Enforcement conducted search operations against Gameskraft Technologies over alleged consumer deception in online rummy gaming.

In **Indonesia**, the Ministry of Communication and Digital Affairs adopted an amended decree updating indicators, technical guidance, and verification procedures for assessing child-related risks in digital products and services. It requires all operators to conduct structured self-assessments across seven risk areas using standardized methodologies and multidisciplinary input. Regarding enforcement, the Ministry blocked access to Polymarket over illegal online gambling activities.

In **South Korea**, the partial amendment to the Copyright Act entered into force, establishing powers for authorities to order the removal and blocking of infringing content, including an emergency blocking mechanism subject to subsequent review, alongside strengthened investigative powers, liability provisions, and penalties. The amendment further provides procedural safeguards, allowing affected parties to file an objection within five days of an emergency blocking measure, during which the block can be lifted while pending review.

Additionally, several bills were introduced to the National Assembly to amend the Telecommunications Business Act, addressing dark patterns, disruptive online advertising, deceptive online practices through design requirements, and interoperability requirements. A further bill would amend the Personal Information Protection Act to prohibit deceptive interface designs.

Regarding **enforcement**, the Fair Trade Commission fined JB International and All That over deceptive trade practices in used iPhone sales and issued improvement recommendations on deceptive pricing and discount practices on online shopping platforms.

Americas

In **Brazil**, the President signed two decrees addressing online safety. The first decree 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. The second decree 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.

The **Canadian** Radio-television and Telecommunications Commission (CRTC) adopted regulatory policies under the modernized Broadcasting Act. The first policy establishes a framework for the discoverability of Canadian and Indigenous content and services, as well as a fund supporting services of exceptional importance. The second policy introduces Canadian programming expenditure obligations for private broadcasting ownership groups and unaffiliated online broadcasting ownership groups with annual revenues of CAD 25 million or more, while exempting groups below this threshold. The policy requires eligible broadcasting ownership groups to allocate at least 25% of their programming and online revenues to Canadian programming, and eligible unaffiliated online broadcasting ownership groups to allocate at least 15% of their online

revenues, including the 5% base contribution established in Broadcasting Regulatory Policy 2024-121. The CRTC also adopted accessibility requirements expanding closed captioning obligations for online streaming services.

Artificial Intelligence

International

The **Group of Seven** (G7) Digital and Technology Ministers adopted a vision document on AI openness, defining it as a spectrum and specifying that systems described as "open" should indicate which components (including weights, code, and training data) are available and under what conditions. It introduces a four-tier typology and encourages its use as a common reference. The Ministers also adopted a declaration on digital and technology cooperation covering secure AI, AI-driven economic growth, digital sector resilience, and efficiency.

Additionally, the G7 Cybersecurity Working Group published minimum elements for a Software Bill of Materials for AI, structured around system metadata, models, datasets, infrastructure, security properties, and performance indicators, to improve transparency across AI supply chains. Separately, the Asia-Pacific Economic Cooperation Trade Ministers adopted the Suzhou Statement, including measures on AI cooperation.

Europe

The **European Parliament** and the Council of the EU reached a provisional agreement on the Digital Omnibus on AI Regulation. Under the agreed text, AI systems that generate non-consensual sexually explicit or intimate content or child sexual abuse material would be prohibited, including their placement on the EU market, deployment for such purposes, or provision without adequate safeguards. The prohibition applies to image, video, and audio outputs, with compliance required by 2 December 2026. The same date applies to watermarking obligations for AI-generated content. It also introduces phased application dates for obligations on high-risk AI systems, including requirements on risk management and human oversight. Obligations for Annex III high-risk systems apply from 2 December 2027, while obligations for Article 6(1) high-risk systems apply from 2 August 2028. Additional amendments cover testing requirements, design requirements, cybersecurity requirements, quality-of-service requirements, data protection provisions, and changes to registration requirements. The provisional agreement remains subject to formal adoption by both institutions before 2 August 2026.

The European Commission opened consultations on two draft guidelines under the AI Act. The first clarifies the classification of high-risk AI systems under Article 6, covering systems used as safety components or products under Annex I harmonization legislation and systems listed in Annex III, as well as the role of intended purpose and potential provider obligations for other actors. The second clarifies transparency obligations under Article 50, requiring users to be informed when interacting with AI systems, mandating technical measures for marking synthetic content, and imposing labeling duties for deepfakes and AI-generated or manipulated content in the public interest, with limited exceptions.

The **German** Federal Commissioner for Data Protection and Freedom of Information published a report on requirements for AI-based medical devices under its AI regulatory sandbox pilot. It

clarifies the additional requirements that developers, manufacturers, and deployers of AI-based medical devices must fulfill, given that medical devices incorporating or constituting an AI system are generally classified as high-risk.

The **Italian** Data Protection Authority closed its investigation into Myndoor without finding established violations but issued a warning that the planned transmission of aggregated stress reports to employers could infringe the General Data Protection Regulation's provisions on data processing, governance, and safeguards, as well as provisions of the EU AI Act prohibiting the use of AI systems to infer emotions in the workplace.

In the **United Kingdom**, the Data Protection Act (Code of Practice on AI and Automated Decision-Making) Regulations entered into force, 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 processing. Separately, the Bank of England, Financial Conduct Authority, and Treasury published a joint statement on frontier AI models and cyber resilience addressed to regulated firms and financial market infrastructures. The statement covers board and senior management oversight of frontier AI risks and measures for protection, response, and recovery, including access controls, network security, data protection, and AI-enabled defenses. Finally, the United Kingdom and Australia signed a memorandum of understanding on AI safety and security.

Asia and Australia

In **Australia**, the Signals Directorate issued guidance on integrating AI into cybersecurity operations. It establishes a framework aligning AI integration across six cybersecurity functions, comprising governing, identifying, protecting, detecting, responding, and recovering, while acknowledging that malicious actors are increasingly leveraging AI to accelerate attacks at greater scale and speed. Additionally, the Securities and Investments Commission issued a letter assessing frontier AI models and their cybersecurity impact for regulated entities. Regarding enforcement, the Office of the Australian Information Commissioner closed its investigation into fastproperty.ai, finding that the platform does not collect, use, or disclose personal information and therefore does not contravene the Privacy Act.

The Cyberspace Administration of **China** (CAC) issued implementation opinions on the standardized application and development of intelligent agents, defining them as systems with autonomous perception, memory, decision-making, interaction, and execution capabilities. The framework applies to consumer, industrial, and public-sector uses across nineteen sectors, including healthcare, transportation, finance, manufacturing, education, government services, and public safety, and provides for tiered governance in sensitive areas with sector regulators responsible for determining permitted use cases and applying measures such as registration, testing, and product recall. The CAC also published the latest generative AI services filing list and deep synthesis service algorithm filing list.

Additionally, the National Computer Network Emergency Response Technical Team announced an initiative on AI cybersecurity testing, and the National Network Security Standardization Technical Committee adopted ethics and safety guidelines for AI applications. The Ministry of Industry and Information Technology also launched a pilot program for ethics review of AI technologies. China

and the United States also announced an intergovernmental dialogue on AI, and China inaugurated the China-ASEAN AI Industry Innovation Center.

In **South Korea**, the Ministry of Science and Information and Communication Technology opened a consultation on an amendment to the Enforcement Decree of the Framework Act on AI. It introduces provisions on AI product and service verification for public procurement, AI research institute procedures, user cost support, and startup financing through venture capital mother funds. Furthermore, a bill amending the local operations requirement under the Framework Act on AI was introduced to the National Assembly, requiring AI business operators without a Korean address or office to report changes to their domestic representative, ensure continuous contactability, and appoint a domestic corporation where available.

The Ministry of Culture, Sports and Tourism issued a guide on fair use for training generative AI, setting out a four-factor assessment covering transformative purpose, nature of the work, extent of use, and market impact, alongside case studies on likely and less likely fair use scenarios. The Financial Services Commission announced measures to ease network separation rules for the use of AI in cybersecurity defense. The Personal Information Protection Commission issued guidance on data privacy risks in generative AI services, including recommendations on opt-out settings, data deletion, and cross-border transfers, and approved Naver's personalized AI search agent service.

The Securities and Exchange Board of **India** (SEBI) issued a circular on cybersecurity risks associated with advanced AI-based vulnerability detection tools, applicable to all regulated entities in the securities market ecosystem. It sets out requirements including prompt system patching with interim virtual patching, regular vulnerability assessments and security audits using conventional and AI tools, vendor risk management, and structured change management. Additionally, India signed a strategic partnership including measures on quantum computing and AI with Italy, a strategic partnership framework on emerging technologies with the Netherlands, and issued a joint statement on an enhanced strategic partnership with Vietnam.

Americas

The Office of the Privacy Commissioner of **Canada** and its provincial counterparts in Quebec, British Columbia, and Alberta issued findings following an investigation into OpenAI's data collection and processing practices. The authorities found that the initial development and deployment of ChatGPT did not fully comply with applicable Canadian privacy laws, citing issues including excessive collection of personal information, insufficient consent, and transparency, among others. In response, OpenAI introduced and committed to additional measures, including reducing the personal and sensitive data used for model training and improving user information on system functionality and privacy implications. The Office of the Privacy Commissioner of Canada concluded that, if fully implemented, these measures address the concerns under the Personal Information Protection and Electronic Documents Act. The Quebec Commission on Access to Information reached a partial resolution, while the Information and Privacy Commissioners of British Columbia and Alberta found consent-related issues unresolved and indicated that they would continue to monitor compliance.

Competition

Europe

In the **European Union**, the Technology Transfer Block Exemption Regulation entered into force, exempting certain technology transfer agreements from the prohibition on anti-competitive agreements under Article 101 of the Treaty on the Functioning of the European Union. It applies to licensing of technology rights, including patents, software copyrights, and know-how, where market share thresholds do not exceed 20% for competitors and 30% for non-competitors, and sets out restrictions such as price-fixing, output limitations, and market allocation.

The European Commission released its third annual report on the implementation of the Digital Markets Act (DMA), covering ongoing investigations into gatekeeper designations and compliance with obligations. Additionally, the Commission also consulted on its specification proceedings to support Google's compliance with DMA's obligations on search data sharing and interoperability.

The Commission also opened an in-depth investigation into JD.com's proposed acquisition of CECONOMY under the Foreign Subsidies Regulation and approved the OpenAI and SoftBank joint venture under the EU Merger Regulation.

Finally, the European Union and Mexico signed the Modernized Global Agreement, which includes provisions requiring both parties to maintain comprehensive competition laws covering anti-competitive agreements, abuse of dominance, and mergers.

In the **United Kingdom**, the Competition Act (Technology Transfer Agreements Block Exemption) Order entered into force, replacing the previous assimilated framework and exempting qualifying technology transfer agreements from the prohibitions regarding anticompetitive agreements. It applies to licensing agreements for technology rights, including patents, software copyrights, design rights, and database rights.

Regarding enforcement, the Competition and Markets Authority (CMA) opened a consultation under its strategic market status investigation into Microsoft's business software ecosystem. The investigation covers productivity software, operating systems, databases, and security software, and considers whether these activities form a single ecosystem and whether AI products such as Copilot fall within scope. It also examines potential competition issues relating to market power, interoperability, commercial bundling and pricing, and default or design choices. Additionally, the CMA conditionally cleared the Getty Images and Shutterstock merger, subject to an editorial-business divestiture, and the Financial Conduct Authority opened an investigation into PayPal over alleged anti-competitive conduct linked to digital wallet funding and usage.

Asia and Australia

The Cyberspace Administration of **China** (CAC) reported initial implementation results of the negative list for algorithms used by lifestyle service platforms across sectors, including food delivery, ride-hailing, logistics, e-commerce, travel, and ticketing. Platforms have introduced 63 measures and committed to 139 requirements covering algorithm design and operation, including order allocation, pricing, and transparency.

Additionally, the State Administration for Market Regulation conditionally approved Tencent's acquisition of an equity stake in Ximalaya, subject to commitments on pricing, service standards, free content, and trading conditions, with ongoing compliance supervision.

The Business Competition Supervisory Commission of **Indonesia** submitted a proposal for a Digital Market Law to Parliament. The proposal introduces requirements on algorithmic transparency, prohibitions on self-preferencing and service discrimination, restrictions on predatory pricing, and obligations on platform cost transparency and AI accountability, alongside inter-agency coordination measures. Furthermore, the Commission imposed a fine of IDR 2 billion on NTT Docomo for breaching merger notification requirements in its acquisition of Intage Holdings.

The Fair Trade Commission of **South Korea** announced an inquiry into competition in the AI service market to assess transaction practices, market structure, and competitive conditions. The inquiry covers 29 AI service developers and 17 AI-enabled product providers and will be conducted in two phases, focusing first on major operators and then on user experiences and usage patterns.

The Supreme Court of **India** allowed Amazon's appeal and set aside the Competition Commission's order and the National Company Law Appellate Tribunal's judgment relating to Amazon's acquisition of a stake in Future Coupons Private Limited. The Court held that the notification requirements were not triggered where prior approval had been granted after review. Additionally, the Delhi High Court issued interim orders in the Commission's investigations into Apple over alleged abuse of dominance in App Store operations and iOS application distribution, recording the Commission's undertaking not to issue final decisions.

Data governance

International

The **Council of Europe** released revised draft guidelines on privacy and data protection for large language model-based systems, addressing risks across the lifecycle from development and adaptation to deployment and user interaction. The guidelines operationalize Convention 108+ principles, including lawfulness, purpose limitation, data minimization, transparency, accountability, and security.

Europe

In the **European Union**, the delegated regulation supplementing the Cyber Resilience Act on notification dissemination delays entered into force. Additionally, the Network and Information Security Cooperation Group adopted common templates for incident reporting under the Directive on measures for a high common level of cybersecurity (NIS2).

Regarding enforcement, at the **member state level**, the data protection authorities of Finland, the Netherlands, and Norway fined Yango EUR 100 million and ordered the cessation of data transfers to Russia in the absence of compliance with the General Data Protection Regulation (GDPR). The Spanish Data Protection Agency resolved its investigation into Konecta following a EUR 300,000 voluntary payment over a data breach. The Belgian Data Protection Authority imposed fines over the improper retention of a former worker's professional mailbox and ruled against Isabel, the

operator of the TruliUs digital authentication and identification service, over its alleged misqualification as a data processor.

In **France**, the National Commission on Informatics and Liberty (CNIL) adopted a recommendation clarifying how lenders and intermediaries should apply data protection rules when assessing an individual's creditworthiness, including in cases where credit scoring and automated decision-making systems, such as AI-based tools, are used.

In the **United Kingdom**, the regulations updating the list of public authorities empowered to request access to communications data under the Investigatory Powers Act framework entered into force.

Asia and Australia

The Office of the **Australian** Information Commissioner opened a consultation on guidance for the automated decision-making transparency obligation introduced by the Privacy and Other Legislation Amendment Act, which is due to commence in December 2026. Large entities will be required to disclose in their privacy policies information about automated systems that make or assist decisions significantly affecting individuals, including the types of data used and decisions made, with the consultation addressing interpretive issues and disclosure scope. Additionally, the Information Commissioner published updated guidance on the collection of solicited personal information.

The Cyberspace Administration of **China** opened consultations on security requirements and cybersecurity labeling rules for consumer-grade connected cameras and on simplified data protection measures for small processors. Regarding enforcement, the Supreme People's Court published information on a RMB 300,000 fine against Bou Software for the unlawful collection of patient registration data.

In **India**, the Delhi High Court upheld the right to be forgotten as part of the right to privacy under Article 21 of the Indian Constitution. It held that search engines act as personal data processors and directed Google and other operators to remove name-based indexing of specified judicial records globally, while distinguishing de-indexing from masking of court documents. The Court set out categories where relief may not apply, including certain convictions and matters involving public figures, and required compliance within two weeks, with directions issued to the Ministry of Electronics and Information Technology to coordinate implementation.

In **Japan**, the Personal Information Protection Commission and the Financial Services Agency opened a consultation on amended guidelines for the protection of personal information in the financial sector.

In **South Korea**, the amended enforcement decree of the Personal Information Protection Act entered into force. It provides that total revenue for calculating administrative fines is based on the higher of the preceding business year's revenue or the average annual revenue of the three preceding years. It also allows the Personal Information Protection Commission (PIPC) to limit or withhold fine reductions at early adjustment stages where a violation is classified as extremely serious. Additionally, two separate bills were introduced to the National Assembly to amend the Personal Information Protection Act. The first bill would enable the PIPC to provide financial and technical support to small-scale processors in areas such as online transactions, platform sales,

and AI training for implementing data safety measures. The second bill would empower the PIPC to impose compulsory enforcement fines, up to 0.3% of average daily turnover, on controllers that fail to submit materials required for investigations.

Furthermore, the Ministry of Science and Information and Communication Technology launched a breach incident investigation review committee, the PIPC adopted a preventive-centered personal information management system transformation plan, and published a personal information dispute mediation casebook. Regarding enforcement, the PIPC announced an inspection into educational technology businesses and confirmed that Incruit, Qookka Entertainment, SK Telecom, KakaoTalk, Naver, Coupang, Baemin, Karrot, and Worldcoin had implemented the corrective measures issued following previous investigations.

Americas

In **Canada**, the Office of the Privacy Commissioner opened consultations on two draft guidelines. The first is addressed to developers on designing age assurance to be privacy-protective and sets out six design requirements, including collecting the minimum information necessary, limiting results to an age range, deleting data once an age signal is generated, and not profiling individuals' age-assured activities. The second is addressed to websites and online services and sets out a three-stage framework requiring them to justify the need for age assurance through a legal requirement or a specific harm to children, choose a proportionate method, and apply it in a privacy-protective manner with method options and appeal mechanisms. The Commissioner also released an accompanying age assurance policy note.

Africa

The Information Regulator of **South Africa** opened a consultation on a draft code of conduct for the processing of personal information at gated access points, including residential, commercial, government, healthcare, and educational sites. The draft sets out obligations for lawful processing, regulates the use of CCTV and biometric technologies, and addresses data collection, retention, security, and deletion, alongside governance, complaints, enforcement mechanisms, and proportionality between security and privacy rights.

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