



Digital Policy Alert

GLOBAL DIGITAL POLICY ROUNDUP

SEPTEMBER 2026



Global Digital Policy Roundup: September 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.

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

- **Content moderation**, including the European Commission's proposal for the KIDS Act setting a minimum age of 15 for social networking and video-sharing accounts, the United Kingdom's announced legislation requiring apps and devices to block nude imagery for children, China's consultation on regulations on minors' internet use, and Brazil's provisional measure banning fixed-odds betting and its advertising.
- **AI regulation**, including the adoption of A Call for Control of Frontier AI Models by 20 governments and the European Union, the G20 innovation ministers' statement on emerging technologies and AI, Italy's decree implementing AI Act provisions on liability, China's AI Safety Governance Framework 3.0, and the introduction of Australia's AI Kill Switch and Data Centre Control Bill.
- **Competition policy**, including the European Commission's adoption of guidelines on exclusionary abuses of dominance, the General Court upholding the prohibition of Booking's proposed acquisition of eTraveli, the Competition and Markets Authority's consultation on a search choice screen for Google that would include AI assistants, the Competition Appeal Tribunal's approval of a £260 million collective settlement with Google, and South Korea's proposal to make acqui-hire transactions reportable.
- **Data governance**, including the entry into effect of reporting obligations under the Cyber Resilience Act and access-by-design requirements under the Data Act, the European Data Protection Board's final guidelines on the interplay between the DSA and the GDPR, Ireland's €403 million fine against Google over location data, and the entry into force of South Korea's amended Personal Information Protection Act.

Content moderation

Europe

The **European Commission** submitted a proposal for the KIDS Act, which would set a minimum age of 15 for creating an account independently on social networking and video-sharing services and introduce safety-by-design requirements. Users aged 13 to 14 would be able to access these services only through a limited account set up by a guardian, with mandatory parental controls such as a daily time limit and contact approval. Children under 13 would not be allowed to hold an account. The proposal would also cover AI companions and chatbots accessible to minors. Providers would have to avoid designs that simulate human relationships in ways likely to foster emotional dependency, assess risks to children before launch, and monitor for harm after deployment. By default, these systems could not retain a child's previous conversations for use in later interactions, and children under 13 could access them only through parental control tools. App stores would be required to support certified EU age-verification solutions, and providers using age-assurance systems would have to meet requirements on accuracy, privacy, non-intrusiveness, and non-discrimination. Very large online platforms would also have to submit age-verification plans. Further, the Commission announced that signatories to the Code of Conduct on Disinformation, including Google, Meta, Microsoft, and TikTok, published their second set of reports under the Digital Services Act (DSA).

At the **member state level**, Poland adopted the Act implementing the DSA, which designates the President of the Office of Electronic Communications as digital services coordinator. In Hungary, a bill was introduced to replace the criteria for classifying programs as harmful to minors, which currently refer to the depiction of identities and sexual orientations, with criteria based on whether content can harm minors' physical, mental, or moral development. A bill was introduced in Bulgaria to ban direct and indirect gambling advertising online. Latvia's Parliament passed the first reading of a 3.5% investment obligation for on-demand audiovisual media services in Latvian-language productions.

Regarding **enforcement**, Ireland's Media Commission opened an investigation into X over the effectiveness of its age assurance mechanisms and parental controls under the Online Safety Code. Hungary's Competition Authority opened a follow-up investigation into TikTok over its 2023 commitments, including default screen time limits and parental controls for users under 18.

In **Germany**, the Frankfurt am Main Regional Court held Meta liable for fake investment advertisements using Finanzfluss's trademark and its founder's image. The court rejected Meta's reliance on the DSA hosting exemption, finding that its algorithms and ad auction process give it control over the content. It ordered Meta to stop distributing the advertisements and to disclose the related revenue.

In the **United Kingdom**, the government announced legislation requiring apps used by children to block access to and sharing of nudity. A second measure would require device and operating system providers to prevent children from taking, sharing, or viewing nude imagery.

The Office of Communications (Ofcom) adopted amendments to the Illegal Content Codes of Practice for user-to-user and search services, recommending hash matching to detect intimate image abuse. Ofcom also issued guidance on the proportion of detected content that should

receive human review. Additionally, Ofcom opened a [call for evidence](#) on implementation of its guidance on women and girls' online safety. It also opened a consultation on a [code of practice for designated radio selection services](#) such as voice assistants.

Regarding **enforcement**, Ofcom fined the provider of [Xgroovy](#) £730,000 for failing to implement highly effective age assurance to prevent minors' access to adult content and to respond to an information request. It opened an investigation into [Aylo](#) over a Pornhub age assurance mechanism that relies on age checks run by Apple. Ofcom also launched an [enforcement program](#) examining whether platforms use hash matching or equally effective measures against non-consensual intimate images and deepfakes. Finally, it opened investigations into [Vonage Business](#) and [Voxbone](#) over suspected failures to prevent scammers from misusing telephone numbers.

Asia and Australia

Australia's Department of Infrastructure and Transport consulted on the [Online Safety Amendment \(Digital Duty of Care\) Bill](#), which would empower the eSafety Commissioner to intervene where platforms fail to adequately self-regulate harmful material. For cyberbullying, intimate images, and abusive material, it would reduce the Commissioner's waiting period from 48 to 24 hours before issuing a removal notice, following which providers would have 24 hours to remove the content.

Further, the Communications and Media Authority opened a consultation on the [Telecommunications \(Consumer Protections\) Industry Standard](#), which would require telecommunications providers to provide pre-sale information, conduct credit assessments, and offer remedies for mis-selling.

In **China**, the regulations on [internet information content multi-channel distribution services](#) came into force. They require platforms to set up complaint channels and to act against multi-channel network organizations that violate laws or platform rules, with measures ranging from warnings to account closure. MCN organizations must [verify the identity](#) of contracted account operators and may not provide live-streaming services to minors under 16. The State Administration for Market Regulation consulted on [compliance guidelines](#) that would require mini-program platforms such as WeChat and Alipay to verify and disclose merchant identities. Finally, the Cyberspace Administration opened a consultation on [regulations](#) on ensuring the healthy and safe use of the internet by minors. The regulations would introduce age-verification requirements and restrict minors' access to certain services, including stranger social networking, virtual intimate relationships, and addictive services, as well as live-stream publishing for users under 16. Providers would also be required to strengthen content moderation, prevent minors' exposure to harmful content, and establish safeguards for users facing serious risks, including self-harm or suicide.

India's Department of Consumer Affairs adopted the Consumer Protection (E-Commerce) (Amendment) [Rules](#), requiring e-commerce entities from January 2027 to label sponsored listings, disclose prior prices when announcing discounts, and refrain from manipulating search results. Entities must also conduct annual self-audits for [dark patterns](#) and display a compliance certificate.

Regarding **enforcement**, the Central Consumer Protection Authority (CCPA) fined [Flipkart](#) ₹1 million and [JioMart](#) ₹500,000 over misleading advertisements and the sale of unregistered

products. It also fined Xboom ₹1 million for misleading advertisements. Over listings of hazardous substances, the CCPA fined Weblink ₹1 million in each of two cases, concerning picric acid and other explosive substances, and fined Dial4Trade Technologies ₹1 million over ammonium nitrate. It further issued directions against ride-hailing platform Namma Yatri over a tipping prompt it found to be manipulative. Separately, the Directorate of Enforcement provisionally attached ₹4.42 billion in assets linked to Gameskraft Technologies over alleged deceptive practices on online rummy platforms.

Indonesia's Ministry of Communication and Digital Affairs announced an enforcement framework for administrative penalties under the child protection regulation. It sets maximum fines of 6% of global revenue for large platforms and up to Rp10 billion for domestic operators. Regarding enforcement, the Ministry requested Meta to speed up the deactivation of accounts belonging to users under 16 on Facebook, Instagram, and Threads, and to prepare an acceleration plan. It also asked Roblox to strengthen its child protection measures.

In **South Korea**, a bill amending the Act on Fair Labeling and Advertising was introduced to the National Assembly to raise the daily non-compliance penalty for failing to implement a Fair Trade Commission (FTC) consent decision from ₩ 2 million to up to 5% of the business's average daily sales. Where a business has no sales or its sales are difficult to calculate, the FTC could impose up to ₩ 20 million per day. Separately, the Personal Information Protection Commission opened an investigation into Google following reports that deletion requests from digital sexual crime victims were allegedly disclosed to external website operators. The investigation will examine whether Google disclosed sensitive personal data without a lawful basis or proper consent and failed to implement adequate safeguards against human error or system failures.

Americas

In **Brazil**, the National Consumer Secretariat (Senacon), together with other agencies, adopted a joint ordinance on paid advertising and content amplification. Providers must offer tools for content creators to disclose material relationships and must store information on each advertisement, including advertiser identity. Providers with over one million monthly active users must also maintain a public, searchable advertising repository. Additionally, the provisional measure no. 1,394 came into force, banning fixed-odds betting and its advertising. It places a duty of care on platforms and app stores to prevent and remove betting content, with fines of up to 10% of revenue in Brazil. The Prizes and Betting Secretariat also adopted an ordinance requiring financial and payment institutions to monitor and block transactions linked to unauthorized betting operators. The National Congress adopted provisional measure no. 1,357, which requires e-commerce platforms in the Federal Revenue Service's compliance program to verify sellers and remove illegal offers. Further, a bill introduced to the Chamber of Deputies would require social media platforms to pause scrolling for five minutes after 30 consecutive videos and display a mental health alert.

Regarding **enforcement**, a task force of the Ministry of Justice and Public Security and the Ministry of Finance took down 506 unauthorized betting websites. The Attorney General's Office asked Google to remove AI-generated fake doctor videos from YouTube and announced the removal of 18 Telegram groups selling counterfeit vaccination passports. Senacon broadened its investigation into Uber and 99 over alleged accessibility failures. The National Secretariat of Digital Rights referred a technical note on the risks of 13 AI companion services for children to the data

protection and consumer authorities. In electoral cases, the Superior Electoral Court held that the deepfake ban applies only to content qualifying as "electoral propaganda." The Regional Electoral Court of Minas Gerais ordered Meta to suspend algorithmic recommendations of a candidate's registered content.

Artificial intelligence

International

G20 innovation ministers adopted a statement on emerging technologies and AI. It encourages pro-innovation frameworks for the trustworthy development and adoption of AI and addresses AI in public services. **Twenty governments** and the European Union, including Australia, Canada, Germany, South Africa, and Türkiye, adopted A Call for Control of Frontier AI Models. It calls for human oversight, pre-deployment testing, and the sharing of information on serious incidents, and invites United Nations members to consider establishing an international body to monitor compliance.

Australia, France, Kenya, and Spain presented the 2026-2027 roadmap of the Coalition for Children's Rights and Protection in the Age of AI. It calls for voluntary action by AI developers and envisages pre-authorization for AI systems that claim to benefit children. At the 4th UNESCO Global Forum on the Ethics of AI, hosted by Saudi Arabia, the co-chairs of the ministerial track issued a statement setting out six non-binding calls to action for implementing the UNESCO Recommendation on the Ethics of AI.

Europe

The **European Commission** opened a consultation on a targeted initiative concerning the copyright framework for European creativity and innovation. It seeks views on copyright issues involving generative AI, online piracy of live events, music remuneration, sound recordings by third-country nationals, and copyright in research.

At the **member state level**, a bill implementing the AI Act was introduced to the Bulgarian Parliament. It would divide market surveillance among sectoral authorities and establish an AI regulatory sandbox.

Regarding **enforcement**, Spain's Data Protection Agency issued a preventive warning to a company planning an AI-based CV screening tool. The agency required a risk assessment, a data protection impact assessment where processing poses a high risk, and effective human oversight before deployment.

In **Italy**, the President signed a decree implementing the EU AI Act provisions on police use of artificial intelligence and civil and criminal liability. It establishes criminal offenses for failing to implement required security measures for high-risk AI systems or altering such systems where this endangers life, public or individual safety, or State security. It also establishes fines and disqualification sanctions for legal entities where specified offenses are committed using AI systems.

In **Russia**, the authority governance provisions of the Law on Supporting the Development of Artificial Intelligence Technologies took effect. They cover presidential approval of the national AI

strategy, government coordination of state support measures, and regional procedures for access to datasets used to train sovereign AI models. The remaining government powers, including the power to set sector-specific risk-prevention requirements, apply from March 2027.

In the **United Kingdom**, the [Artificial Superintelligence Bill](#) was introduced to the House of Commons. It would prohibit the development and operation of superintelligent AI systems and [empower the government](#) to restrict systems identified as precursors. The [Personal Data \(Digital Twins\) Bill](#) would require explicit consent before a digital twin of an individual is created and would prohibit digital twinning of children. Further, the Department for Business and Trade closed its consultation on [workplace monitoring technologies](#), including AI-based algorithmic management. The consultation set out options ranging from a statutory code of practice to non-statutory guidance.

Asia and Australia

The AI Kill Switch and Data Centre Control Bill was introduced to **Australia's** House of Representatives. It would require providers of advanced AI systems to maintain the capability to [stop inference and shut down systems](#), conduct [red-teaming](#), and [report critical incidents](#) to the Minister within 24 hours. The bill would also empower the Minister to [issue emergency directions](#) and impose a [moratorium](#) on new AI data center construction. Additionally, the Signals Directorate issued [guidance](#) on securing agentic AI harnesses through least-privilege access, audit logging, and human oversight of high-impact actions.

China's National Cybersecurity Standardization Technical Committee released the [AI Safety Governance Framework 3.0](#), which classifies AI risks as inherent, application, or derivative risks and sets out corresponding technical countermeasures and a regulatory sandbox mechanism. The Supreme People's Court issued an [opinion](#) on adjudicating AI disputes. It holds that generative AI use of names, images, or voices without consent infringes personality rights. It requires providers to stop generating infringing content upon notification or bear joint liability, and attaches tort liability to algorithmic price discrimination. Finally, the Cyberspace Administration published [filing information](#) for 124 generative AI services registered in July and August 2026, bringing the total to 1,112 registered services.

Japan's [guidelines for government procurement of generative AI](#) came into force. Contracted vendors must maintain AI governance frameworks, incident response procedures, harmful content controls, and security measures against prompt injection. The Ministry of Economy, Trade and Industry also opened a [call for case examples](#) to inform revisions to the guideline on AI and data usage contracts.

In **South Korea**, the President promulgated amendments to the [Personal Information Protection Act](#), effective March 9, 2027. The amendments allow lawfully collected personal information to be used for AI development beyond its original purpose, subject to approval and supervision by the Personal Information Protection Commission (PIPC). Additionally, a [bill](#) amending the AI Basic Act was introduced to the National Assembly. It would require operators of conversational AI to ensure that users recognize during conversation that they are interacting with AI.

Regarding **enforcement**, the PIPC issued corrective recommendations to three AI companies. [OpenAI](#) received one over complaints to its domestic representative that went unanswered.

DeepSeek received one for providing rights-exercise guidance only in Chinese. Wrtn Technologies received one over its failure to respond to data subject requests.

Americas

A bill was introduced to the Chamber of Deputies of **Argentina** to require high-risk AI systems to be entered in a public registry before being placed on the market. Registration would require a published human rights impact assessment developed with affected stakeholders.

Competition

Europe

The **European Commission** adopted guidelines on the application of Article 102 of the Treaty on the Functioning of the European Union to exclusionary abuses of dominance. They cover conduct such as predatory pricing, exclusive dealing, and refusal to supply, and address dominance assessments involving ecosystems and after-markets.

Regarding **enforcement**, the Commission announced that Booking made voluntary changes following a regulatory dialogue under the Digital Markets Act (DMA). Booking no longer considers prices set through other sales channels when deciding whether a property is eligible for its Sponsored Benefit program.

At the **judicial level**, the General Court upheld the Commission's prohibition of Booking's proposed acquisition of eTraveli. It found that the transaction would have strengthened Booking's dominant position in hotel online travel agency services through its "connected trip" strategy. The General Court also dismissed Opera Norway's challenge to the Commission's decision not to designate Microsoft Edge as a gatekeeper service under the DMA.

At the **member state level**, the Dutch House of Representatives passed a bill that would allow the Authority for Consumers and Markets to call in concentrations below the notification thresholds where one party has a turnover of at least €50 million in the Netherlands, and it would expand the Authority's information-gathering powers. Spain's National Markets and Competition Commission (CNMC) concluded its inquiry into cloud services. It found that Amazon and Microsoft account for 60% to 70% of certain segments and identified vendor lock-in and data egress fees as competition concerns. The CNMC recommended a closer assessment of the sector, including extending the DMA to cloud services.

In **Germany**, the Federal Government introduced the twelfth amendment to the Act Against Restraints of Competition to Parliament. The amendment would raise the merger control turnover thresholds and widen the €400 million transaction value threshold to cover targets expected to become active in Germany. For those cases, it would introduce a simplified notification procedure. The amendment would also extend the right to a Federal Cartel Office decision on cooperation to vertical agreements and widen the cartel prohibition exemption to cover cooperation between private broadcasters.

In the **United Kingdom**, regulations under the Digital Markets, Competition and Consumers Act extended transitional arrangements for alternative dispute resolution providers until January 7,

2027. The Office of Communications opened a consultation on revised [enforcement guidelines](#) for Competition Act investigations, which reflect new powers under the Digital Markets, Competition and Consumers Act and update the settlement procedure.

Regarding **enforcement**, the Competition and Markets Authority (CMA) opened a consultation on revised [user choice conduct requirements](#) for Google, which holds strategic market status in general search. Under the proposals, Google would have to display a search provider choice screen on Android devices and in Chrome, and AI assistants would be eligible to appear on it. A related [attribution obligation](#) would require Google to ensure that search providers on the choice screens credit the publisher content they rely on. Separately, the Competition Appeal Tribunal approved a collective settlement under which [Google](#) will pay £260 million without admitting liability. The proceedings, brought on behalf of United Kingdom app developers, concerned alleged abuse of dominance in Android app distribution, including Play Store commissions of up to 30%.

Asia and Australia

The **Australian** Competition and Consumer Commission accepted an undertaking from [REA Group](#), operator of an online platform where real estate agencies list residential properties for sale and rent. REA will stop requiring real estate agencies to list all or most of their properties on its platform as a condition of accessing services or sponsorship.

South Korea's Fair Trade Commission (FTC) consulted on [amendments](#) to the business combination notification guidelines that would make acqui-hire transactions in fields such as AI reportable. The amendments would address transfers of personnel valued at 10% or more of the transferring company's total assets or at least ₩10 billion. They would count all economic consideration, including intellectual property licenses and non-compete waivers, toward the transfer value.

Regarding **enforcement**, the FTC began a pre-review of [Uber's proposed acquisition of Delivery Hero](#), which would give Uber control of the delivery platform Baemin. It will assess effects on the taxi-hailing and delivery app markets. The FTC also announced deliberation proceedings in a bid-rigging case against [four tablet manufacturers](#) over digital textbook procurement bids worth approximately ₩65 billion. The investigator recommended corrective orders, surcharges, and criminal referral.

Americas

In **Brazil**, the Administrative Council for Economic Defense (CADE) closed its investigation into [Amazon's investment in Anthropic](#) without finding infringements. It concluded that the transaction did not meet notification thresholds and that the companies' agreements did not constitute associative contracts. CADE also approved [B3's acquisition of a 60% stake in CRDC](#) subject to a concentration control agreement. The agreement prohibits tying, sets interoperability obligations, and bars B3 from acquisitions of competitors that would give it over 20% of the voting capital in the markets for registering duplicate invoices, bank credit certificates, and rural product certificates until the end of 2029. It also requires B3 to notify CADE of any transactions with competitors or registration and bookkeeping agents until the end of 2030.

Data governance

Europe

The manufacturers' reporting obligations under the **European Union's Cyber Resilience Act** took effect. Manufacturers must report actively exploited vulnerabilities and serious incidents through the Single Reporting Platform operated by the EU Agency for Cybersecurity (ENISA). The access-by-design requirements of the Data Act also became applicable to connected products and related services placed on the market after September 12, 2026.

The Commission adopted an implementing regulation on minimum metadata elements for health datasets made available for secondary use, applicable from March 2029. The Commission also proposed a Regulation on public contracts and concessions. It would require eProcurement service providers to store procurement data within the European Economic Area and would integrate Cyber Resilience Act cybersecurity requirements into procurement. Further, the Commission opened a consultation on a regulation on minimum performance standards for data centers, covering energy efficiency, water use, and waste-heat reuse.

The European Data Protection Board (EDPB) adopted final guidelines on the interplay between the Digital Services Act and the General Data Protection Regulation (GDPR). They cover notice-and-action mechanisms, deceptive design, advertising transparency, recommender systems, and the protection of minors. The EDPB also opened a consultation on guidelines on imposing administrative fines relative to other corrective powers. The draft sets out a five-step method under which minor infringements generally lead to a reprimand rather than a fine.

Regarding bilateral agreements, the European Union and the Philippines reached substantial agreement on a Free Trade Agreement that includes data protection provisions that would facilitate cross-border data flows. The European Commission submitted proposals for Council Decisions on the signing and conclusion of the EU–India Free Trade Agreement, which provides for cooperation on cybersecurity incidents and digital identity interoperability.

At the **judicial level**, the Court of Justice ruled that the GDPR precludes national legislation requiring online disclosure of shareholders' personal data without access conditions. In two opinions, Advocates General found Belgian data retention rules incompatible with the ePrivacy Directive, and found consent given for unidentified "partners" invalid for electronic direct marketing.

At the **member state level**, an amendment requiring the Dutch Data Protection Authority to publish GDPR sanction decisions came into force. The Estonian Parliament adopted amendments to the Cybersecurity Act introducing near-miss reporting and targeted security audits of essential entities. Spain closed a consultation on a Royal Decree that would require operators of data centers with a capacity of 1 megawatt or more to be established in the EU and keep operational data there.

Regarding **enforcement**, Ireland's Data Protection Commission fined Google €403 million over unlawful processing of location data in its Web & App Activity, Location History, and Location Accuracy features, and ordered compliance within six months.

In the **United Kingdom**, the Information Commissioner's Office (ICO) approved a code of conduct for information-sharing protocols among public and third-sector organizations in Wales. Regarding enforcement, the ICO announced that TikTok withdrew its appeal against the £12.7 million fine over its processing of children's data, making the penalty final. TikTok also withdrew its appeal against an information notice, allowing the ICO's investigation into its recommender systems' use of data on users aged 13 to 17 to proceed. Separately, Grindr agreed to pay £26 million to settle a group action over alleged privacy violations, without admission of liability.

Asia and Australia

Australia's Attorney-General's Department closed its consultation on the Privacy Amendment (Personal Data Protection) Bill. The bill would introduce a fair and reasonable test for collecting, using, and disclosing personal information. It would extend the definition of personal information to cover AI-generated inferences and add precise geolocation to sensitive information, and it would give users of large digital platforms a right to erasure. It also contains security and destruction obligations and provisions on authority governance. Entities would have to regularly evaluate the effectiveness of their security and destruction measures and notify the Information Commissioner of eligible data breaches within 72 hours.

In **China**, the Cyberspace Administration's simplified measures for processors handling data on fewer than 100,000 people came into force. These processors may publish a shortened privacy notice instead of notifying individuals, carry out compliance audits every five years instead of every two, and use simplified impact assessment templates. Sensitive personal information still requires separate notification and consent.

Japan's Personal Information Protection Commission presented policy considerations for the Cabinet Order and Rules implementing the amended Act on the Protection of Personal Information. They cover consent exceptions, the rights of minors under 16, and advance notice before collecting facial recognition data. The Commission also proposed revising its general guidelines to add examples of cybersecurity measures.

In **South Korea**, the amended Personal Information Protection Act came into force. It designates business owners as ultimately responsible for data protection, extends breach notification obligations, and allows surcharges of up to 10% of total sales for repeat or large-scale violations. An amendment to the enforcement decree of the Personal Information Protection Act also entered into force. It requires breach notification within 72 hours and board approval for large processors' chief privacy officers. Three bills were introduced to the National Assembly. Two would sanction the concealment or destruction of investigation materials, and a third would require processors to revoke access rights when personnel change duties. The Personal Information Protection Commission (PIPC) opened a consultation on certification examination methods.

Regarding **enforcement**, the PIPC issued corrective recommendations to Tesla Korea for providing rights-exercise guidance only in English. It also issued recommendations to Roborock, Samsung, LG, Ecovacs, and Xiaomi over data handling in robot vacuum cleaners.

Americas

The **Brazilian** Central Bank adopted Resolution No. 587 amending the Pix payment scheme. It requires participants to notify account holders of security incidents involving personal data from

February 2027. Additionally, participants may flag users if they have a well-founded suspicion of fraud, after which they must reject all Pix transactions involving those users, except refunds. Flagged users must be informed and can request a review.

Canada's Office of the Privacy Commissioner opened a consultation on guidance for assessing third-party service providers that handle personal information. Regarding enforcement, the Office of the Privacy Commissioner opened an investigation into IDScan over a data breach involving driver's license scans.



Contact
Written by Maria Buza and Şeymanur Yönt Gökçen
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

