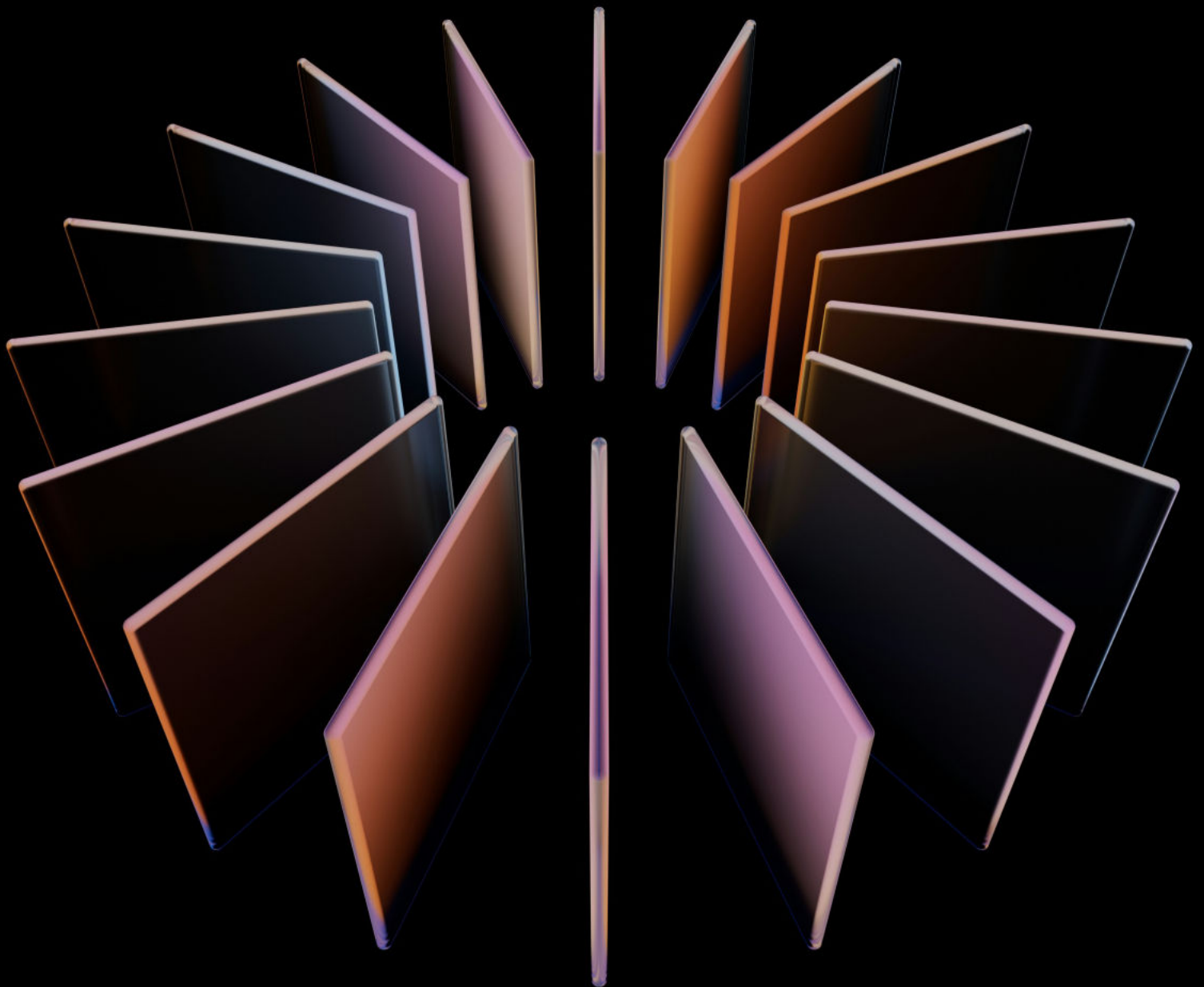


GENTEMIZER

Two-Minute Recap

Data Protection Law Matters Around the Globe

2026 January



EU and Brazil Adopt Mutual Data Protection Adequacy Decisions

On 27 January 2026, the European Union and Brazil adopted mutual adequacy decisions, confirming that Brazil's data protection framework provides a level of protection essentially equivalent to the GDPR. The decisions allow the free flow of personal data between the EU and Brazil without additional transfer safeguards, such as standard contractual clauses. Together, they create the largest area of free and secure data flows globally, covering around 670 million individuals.

The adequacy findings follow a positive opinion from the European Data Protection Board and approval by EU Member States. The European Commission will review the adequacy decision after four years, in line with the GDPR.

ICO Issues Updates on Data Transfers and Enforcement

In the first weeks of 2026, the UK Information Commissioner's Office ("**ICO**") published a series of updates affecting international data transfers and enforcement practice under the UK GDPR. In particular, the ICO:

- » On 15 January 2026, it updated its guidance on international data transfers under the UK GDPR, clarifying how organisations should assess whether a restricted transfer occurs. The guidance confirms that the assessment

should focus on the contractual location of the recipient organisation rather than the physical location of the data, meaning that a restricted transfer may arise even where personal data does not leave the UK. It also reiterates that responsibility for safeguards lies with the party that initiates the transfer, confirms that remote access can constitute a transfer, and clarifies that transfers from a UK-based processor to its overseas controller do not qualify as restricted transfers.

- » On 8 January 2026, the UK Government signed a memorandum of understanding with the ICO, thereby establishing a framework for cooperation on data security. This framework included sharing information and learning from personal data breaches, whilst ensuring the ICO's regulatory independence was not compromised.

Taken together, the updates suggest a more practical, structured regulatory approach, with greater focus on clarity, proportionality, and early engagement with organisations.

California's Delete Request and Opt-Out Platform Became Available

California's Delete Request and Opt-Out Platform ("**DROP**"), a centralised tool that allows residents to submit a single opt-out and deletion request to data brokers, was made available to state residents on 1 January. Since its launch, more than 215,000 residents have signed up. The California Privacy Protection Agency oversees the platform and currently includes 545 registered data brokers. Deletions are set to begin in August,

while regulators have warned that data brokers may face daily fines for non-compliance.

California Fines Data Broker Over Sensitive Health Data Sales

On 13 January 2026, the California Privacy Protection Agency fined Texas-based data broker Rickenbacher Data LLC (Datamasters) USD 45,000 and banned it from selling Californians' personal data. The CPPA found that the company traded highly sensitive health data and failed to register as a data broker as required under California's Delete Act, highlighting stricter enforcement against unlawful data brokerage practices.

Australia Launches First Privacy Sweep on In-Person Data Collection

Australia's privacy regulator, the Office of the Australian Information Commissioner ("**OAIC**"), launched its first privacy sweep in January,

targeting the in-person data collection practices of around 60 organisations across sectors such as rentals, pharmacies, venues, and car dealerships.

The sweep reflects the OAIC's stronger enforcement powers under the amended Privacy Act and focuses on transparency, data minimisation, and deletion practices. Results and possible enforcement actions are expected in the coming months, signalling a more assertive approach to privacy enforcement in Australia.

Spanish Airport Operator Aena Challenges €10 Million Data Protection Fine

Spain's airport operator Aena has announced that it will appeal a €10 million fine imposed by the Spanish Data Protection Authority over the use of facial recognition systems at airport boarding gates. The case focuses on Aena's use of passengers' facial images to verify identity during boarding and whether the company adequately assessed the privacy risks before rolling out the system. According to the regulator,

Aena did not carry out a proper assessment of how the processing of biometric data could affect passengers' privacy, even though such data is subject to stricter protection under the GDPR. Aena has rejected this view, arguing that facial images were encrypted, stored locally on devices, and deleted after boarding, and that no data breaches have been reported since the systems were introduced in 2023. While the appeal is ongoing, at least one major airport operated by Aena has reverted to manual document checks, adding several minutes to boarding times and illustrating the real-world impact of data protection enforcement.

WhatsApp Channels Face New EU Platform Obligations

In late January, the European Commission formally designated WhatsApp's *Channels* feature as an "extensive online platform" under the Digital Services Act, after it was found to have more than 45 million average monthly users in the EU. The designation does not affect WhatsApp's private messaging service, but it does bring Channels within the Digital Services Act ("DSA")'s stricter transparency and risk-management obligations. As a result, Meta will be required to take additional steps to address illegal and harmful content on Channels and to provide greater oversight of how the feature operates. While the decision sits within the DSA framework, it has also prompted discussion about the potential knock-on effects for user data and privacy, given the scale of monitoring and data handling that may be required to meet the new obligations.

Kazakhstan Proposes Criminal Sanctions for Major Data Breaches

In January, Kazakhstan signalled a stricter approach to personal data protection by proposing new criminal and administrative penalties for large-scale data breaches. Government officials announced plans to introduce criminal liability for serious personal data leaks, alongside significantly higher fines for organisations that fail to comply with data protection and information security requirements. The proposed measures would apply across both the public and private sectors, including government bodies, financial institutions, and companies handling large volumes of personal data. The initiative follows a series of high-profile breaches in recent years, including incidents affecting millions of individuals, and reflects growing concern over the scale and impact of data leaks. If adopted, the reforms would mark a significant shift in Kazakhstan's enforcement framework by moving beyond administrative sanctions and placing greater personal and corporate responsibility on data handlers.

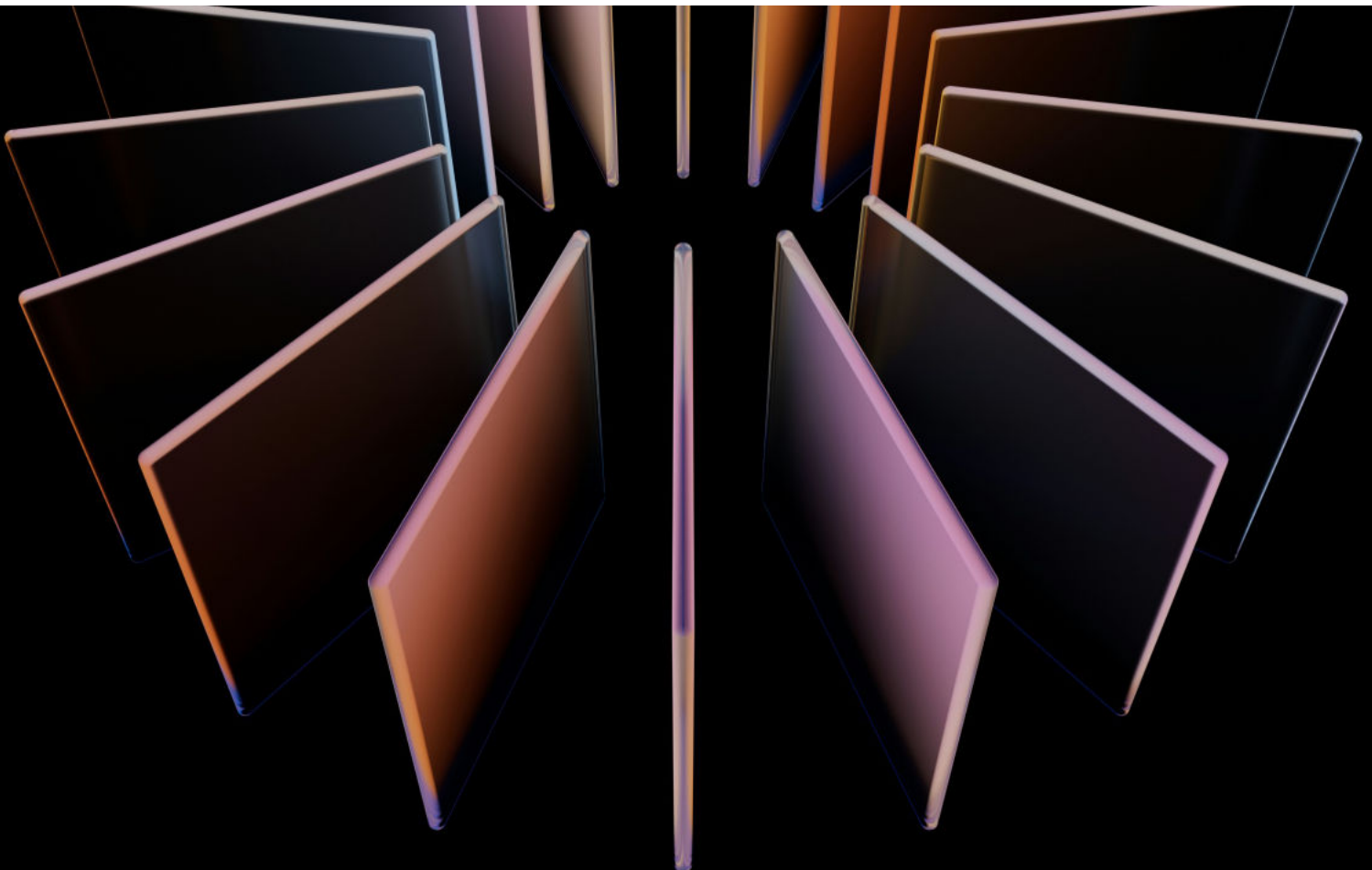
CNIL Fines Free and Free Mobile €42 Million Over Major Data Breach

On 13 January 2026, France's data protection authority ("CNIL") fined telecoms operators

Free Mobile and Free a combined €42 million following a large-scale data breach affecting around 24 million subscriber accounts. The investigation found that basic security measures were lacking, allowing attackers to access sensitive personal data, including IBANs, and that affected individuals were not adequately informed about the consequences of the breach or the steps they could take to protect themselves. The CNIL also criticised Free Mobile for retaining former customers' data for far longer than necessary, in breach of the GDPR's storage-limitation principle. Alongside the financial penalties, the companies were ordered to complete a series of remedial measures, reinforcing the CNIL's message that fundamental GDPR obligations around data security, breach notification, and data retention remain a central focus of enforcement.

EU Considers US Access to Biometric Databases

EU states are preparing to grant US officials direct access to national biometric databases containing fingerprints and facial profiles, in a delayed quid pro quo for maintaining visa-free travel. The Commission is set to lead framework talks in 2026 under Enhanced Border Security Partnerships. According to an EU negotiation document, this framework could allow the transfer of special categories of personal data, provided it is necessary, and safeguards are in place. The European Data Protection Supervisor has warned that this could set an important precedent and has stressed the need for limits and protections.



GenTemizer is a Turkish law firm based in Istanbul, Türkiye. We advise various businesses in relation to their investments, M&A, competition law/antitrust, project financing and construction projects as well as on operational and dispute resolution matters in the context of the Turkish regulatory framework. We have also advised investors in relation to government sponsored privatisation projects.

We are listed in *Legal 500*, *IFLR1000* and *Chambers and Partners* as one of the leading law firms in Türkiye. Each of our partners have also been recognised as one of the leading lawyers in Türkiye. We understand and can meet the demanding requirements and innovative, responsive thinking required for an investment transaction in Türkiye.

For more information, you can contact us.



Ebru Temizer

Partner

etemizer@gentemizer.com



Sinan Abra

Counsel

sabra@gentemizer.com



Irmak Seymen Varat

Managing Associate

iseymen@gentemizer.com



Seray Apak Başaran

Associate

sapak@gentemizer.com



Lorin Tutci

Legal Trainee

ltutci@gentemizer.com



Filippa Angelaki

Legal Trainee

fangelaki@gentemizer.com