

DATA PRIVACY AND PROTECTION

INTRODUCTION

Welcome to the inaugural edition of Babalakin & Co.'s Data Privacy Digest. This digest is a trusted resource for navigating the dynamic and evolving landscape of data privacy and protection law. As we launch this digest, we bring you expert insights, industry trends, and critical updates from January to August 2025, all aimed at helping businesses and individuals stay ahead in the increasingly complex world of data governance.



In a time when data is both a powerful asset and a potential liability, understanding the intricate legal frameworks surrounding its protection has never been more vital. The first half of 2025 has seen landmark developments in regulatory enforcement, judicial decisions, and technological advancements that are shaping how data privacy laws are interpreted and applied. From emerging trends in artificial intelligence to the ongoing evolution of data protection laws across jurisdictions, this digest will provide you with a comprehensive overview of the most significant issues in the data privacy space.

As always, our aim is to empower our clients, partners, and stakeholders with the knowledge needed to navigate the complexities of data privacy, mitigate risks, and ensure compliance with both local and international data protection standards. We invite you to explore this edition, where we dive deep into key developments, share expert commentary, and provide actionable insights that will help you stay compliant and competitive in today's data-driven world.



Enjoy the read and stay informed.

Regulatory Updates

NDPC issues General Application and Implementation Directive (GAID) 2025
On 20 March 2025 the Nigeria Data Protection Commission (NDPC) issued the General Application and Implementation Directive (GAID), replacing the Nigeria Data Protection Regulation (NDPR) and its implementation Framework (NDPRIF) and providing a



six-month transition period ending 19 September 2025. The directive requires Data Controllers and Processors of Major Importance to register, conduct compliance audits and file audit returns; clarifies roles for data protection officers; introduces filing fees; and details cross-border transfer rules and data subject rights. **Read more** [here](#).

Enforcement Actions

Nigeria Data Protection Commission (NDPC) probes Data Compliance across Key Sectors



On 25 August 2025, the NDPC via a public notice announced a sector-wide investigation targeting 1,369 organisations in pensions, gaming, banking, insurance, and insurance brokerage sectors for

possible violations of the Nigeria Data Protection Act (NDPA). The affected Companies have 21 days to file compliance returns, appoint data protection officers, demonstrate technical and organisational measures, and provide evidence of registration as a Data Controller or Processor of Major Importance or face enforcement action. **Read more** [here](#).

NDPC Enters into Deep Collaboration with Independent Corrupt Practices and Other Related Offences Commission (ICPC)



The NDPC has entered into deeper collaboration with Nigeria's anti-corruption agency ICPC. This partnership aims to enhance data protection across public institutions, using data security as a frontline defense against fraud and corruption. A formal Memorandum of Understanding (MoU) is expected to follow soon. **Read More** [here](#).

Surfshark Report Highlights Breach Trends



Cybersecurity firm Surfshark reported that over 150,000 Nigerian accounts were compromised in the first half of 2025. Breaches dropped 73% between Q1 (120,000 incidents) and Q2 (31,800 incidents), yet Nigeria has experienced 23.3 million breached accounts since 2004; roughly one tenth of Nigerians have faced a breach. **Read more** [here](#).

Multichoice Nigeria fined for Violating the Nigeria Data Protection Act



The NDPC fined Multichoice Nigeria ₦766.2 million after a 2024 investigation found intrusive data processing and unlawful cross-border transfers. The company's remediation was deemed unsatisfactory, and the penalty is the largest yet imposed by the NDPC. **Read more [here](#).**

Case Law

Omotayo v Airtel Networks

A Lagos subscriber, Mr. Dayo Omotayo, sued Airtel for allegedly disclosing his call records to a third party. The High Court dismissed his claim, but the Court of Appeal reversed this decision. The appellate court held that the relationship between telecom providers and subscribers is governed by statutory provisions (like the Nigeria Communications Act) and the Constitution, not just standard SIM-card contracts.



It emphasised that call records fall under the constitutional guarantee of "privacy of correspondence and telegraphic communications," meaning that telecom providers must keep customers' personal information confidential and obtain their consent before any disclosure. **Read more [here](#).**

Incorporated Trustees of Personal Data Protection Awareness Initiative V. Nizamiye Hospital Limited Clarifies Locus and Consent

The Incorporated Trustees of Personal Data Protection Awareness Initiative filed a public-interest suit against Nizamiye Hospital, alleging that the hospital unlawfully captured CCTV images, conducted surveillance and failed to warn patients of the consequent data use.



The Federal High Court of Nigeria, heard the suit and in its considered ruling delivered on 10 April 2025, held that it found no substantive breach because consent was given by the patients and CCTV served a security purpose. The case underscores the need for clear privacy notices. **Read more [here](#).**

International Highlights

European Union (EU): Data Act to boost industrial data sharing

The EU's **Data Act**, published in December 2023, came into force on from **12 September 2025**. It aims to make industrial and Internet of Things (IoT) data more accessible and usable by clarifying who can use what data and under what conditions,



giving IoT users greater control, protecting against unfair contractual terms and creating mechanisms for public-sector access while safeguarding against unlawful foreign government requests. **Read more [here](#).**

European Union: Pseudonymised data may not always be personal – CJEU decision



In September 2025, the Court of Justice of the European Union clarified that pseudonymised data is not automatically personal data for every party; whether it is personal depends on the recipient's ability to re-identify individuals. The court held that personal opinions are personal data and that data subjects must be informed if pseudonymised data may be transferred. The ruling emphasises context-based assessments and transparency obligations. **Read more [here](#).**

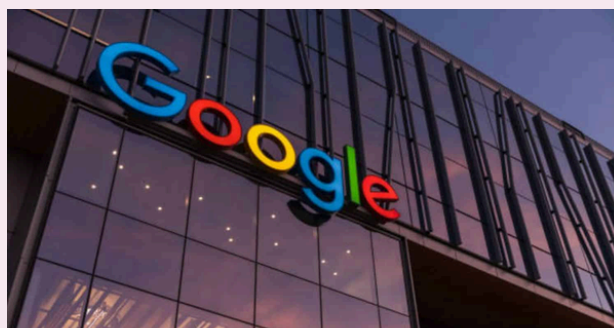
United Kingdom: Data (Use and Access) Act 2025 reforms UK GDPR



The UK's **Data (Use and Access) Act (DUAA)**, enacted on **19 June 2025**, amends the Data Protection Act 2018 and UK GDPR. It introduces a list of "recognised legitimate interests," expands research definitions, eases cookie rules, streamlines data-subject access requests, allows broader use of automated decision-making under safeguards, and phases in reforms between June 2025 and June 2026. **Read more [here](#).**

United States: Jury orders Google to pay \$425 million

A federal jury in California found that Google collected user data despite users disabling the "Web & App Activity" setting and ordered the company to pay \$425 million in damages. The verdict covers about 98 million users and 174 million devices and adds to growing jurisprudence holding tech firms accountable for opaque data practices. **Read more [here](#).**



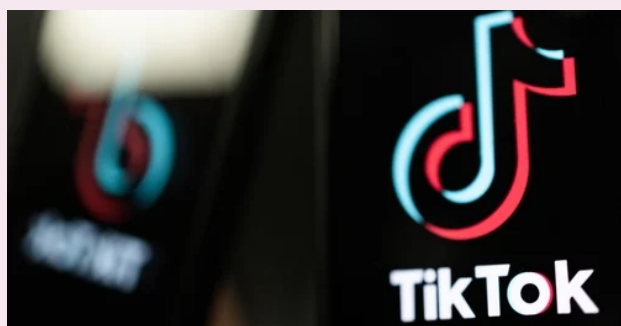
United States: Meta's \$725 million settlement upheld on appeal

Meta Platforms, the parent company of Facebook, urged a U.S. appeals court to uphold a \$725 million class-action settlement resolving claims that Facebook shared user data with third parties like Cambridge Analytica. The settlement, approved by a lower court in 2023 and challenged by some users, is one of the largest data-privacy payouts. **Read more [here](#).**



Ireland: TikTok fine on cross-border access & enforcement

In May 2025 Ireland's Data Protection Commission (DPC) issued a €530 million fine against TikTok, citing failures in protecting EU user data from access by staff in non-EEA jurisdictions and weaknesses in the company's transfer safeguards. The case underscores the EU's intolerance of inadequate technical and organisational measures where data can be accessed remotely by personnel outside the EU,



and it highlights that transfer risk is not only a contractual question but an operational one (who actually can access data, from where). For multinational platforms and data processors, the TikTok decision should prompt immediate technical audits (remote access controls, logging, privileged access management) and legal re-assessments of transfer mechanisms. **Read more** [here](#).

South Africa: Mandatory online breach reporting

From 1 April 2025, all South African organisations must report data breaches through the Information Regulator's eServices portal, replacing email reporting.



Reports must be made promptly to the regulator and affected individuals, and guidance for registration and reporting has been published. **Read more** [here](#).

South Africa: Truecaller under investigation



South Africa's Information Regulator is investigating Truecaller after complaints that the caller-ID app mislabels legitimate numbers as spam and charges businesses a fee to be whitelisted. The investigation will assess whether Truecaller's crowd-sourced model complies with the Protection of Personal Information Act (POPIA) and whether its whitelisting fees are unfair. **Read more** [here](#).

India: Draft Digital Personal Data Protection Rules 2025

India's Ministry of Electronics and IT released draft rules under the Digital Personal Data Protection Act on 3 January 2025, open for consultation until 18 February 2025. The rules propose clear notice requirements, explicit consent, baseline security measures (including encryption and anonymisation) and mandatory breach notification within 72 hours. They also address parental consent for children's data and data-erasure obligations. **Read more** [here](#).



EDPB Clarifies GDPR–DSA Interplay with New Guidelines

The **European Data Protection Board (EDPB)** adopted **Guidelines 3/2025** on 11 September 2025, explaining how the **Digital Services Act (DSA)** aligns with GDPR. The guidelines address lawful bases, data minimisation, and transparency in cases where



online platforms process personal data to meet DSA obligations. **Read more** [here](#).

ANPD Releases Brazil's 2025-2026 Regulatory Agenda Prioritising AI, Biometrics, & Rights Expansion

The Brazil's National Data Protection Authority (ANPD) announced its 2025-2026 regulatory agenda. The agenda includes plans for new regulation or guidelines on artificial intelligence, biometric data, strengthening data subject rights, and improving clarity over international data transfers. This reflects Brazil's growing role in the global data protection landscape and increasing regulatory ambition. **Read more** [here](#).



European Commission and Brazil Advance Towards Mutual Adequacy Decision



On 5 September 2025, the European Commission announced the launch of the process to adopt an adequacy decision with Brazil under the General Data Protection Regulation (GDPR), determining that Brazil ensures an adequate level of personal data protection comparable to that in the EU. Once adopted, the decision would permit personal data to flow freely between Brazil and the EU without the need for additional safeguards, covering flows from businesses, public authorities, and research projects. **Read more** [here](#).

Canada's Proposed Federal Privacy Reform (Bill C-27) Dies, Provinces Fill the Gap

In early 2025, Canada's planned overhaul of federal privacy law under Bill C-27 (which would have created the Consumer Privacy Protection Act and Artificial Intelligence & Data Act) stalled when Parliament was prorogued.



As a result, the older PIPEDA remains in place, while provinces (notably Québec) are progressively implementing stronger privacy and AI-related frameworks to compensate. Legal professionals view 2025 as a period of uncertainty and transition. **Read more** [here](#).

OPC Launches Children's Privacy Framework Consultation in Canada

In May 2025, the Office of the Privacy Commissioner of Canada (OPC) initiated a public consultation to develop a **Children's Privacy Framework**. The goal is to clarify obligations for private-sector entities when processing data of minors, particularly around consent, profiling, and transparency. This is part of the rising importance of child data protections in Canada post-Bill C-27. **Read more** [here](#).



Brazil ANPD Issues Technical Note on AI & Automated Processing



The ANPD published **Technical Note No. 12/2025/CON1/CGN/ANPD** following a public consultation (Nov 2024 – Jan 2025) focused on automated processing and AI use. The note provides regulatory considerations for controllers and processors using AI/automated decision-making. **Read more** [here](#).

Mexico: New Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP) Enacted

Mexico overhauled its private-sector privacy framework with the **new Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP)**, published 20 March 2025 and effective 21 March 2025.



The law replaces the 2010 regime, tightens consent and transparency obligations, expands data-subject rights, updates rules on cross-border data transfers, and shifts supervisory architecture (including institutional changes to oversight). Companies operating in Mexico must update notices, contracts, and transfer mechanisms to align with the new law.

Argentina: Personal Data Protection Bill (S-0644/2025)

Argentina's Senate received Bill **S-0644/2025 on 5 May 2025**, proposing modernised rules on personal data protection, including clearer limits and procedures for public-authority access to personal data (principles of necessity, proportionality and judicial authorisation in many cases). The bill aims to strengthen privacy safeguards while clarifying government access pathways, it remains in parliamentary consideration and will affect



public-sector processing rules if enacted. **Read more** [here](#).

Singapore (PDPC): Personal Data Protection Week 2025 — AI Tools, PETs & Global AI Assurance Sandbox

The **Personal Data Protection Commission (PDPC)** held Personal Data Protection Week in July 2025, launching practical resources including PETs Adoption Guides and promoting the Global AI Assurance Sandbox to help organisations responsibly adopt AI while managing privacy risk. Singapore continues to provide sectoral guidance and practical tools rather than wholesale legislative rewrites. **Read more** [here](#).



South Korea: PIPA Amendment Passed by National Assembly for Stronger Domestic Representative Regime & AI Provisions

On 13 March 2025, South Korea's National Assembly approved amendments to the Personal Information Protection Act (PIPA) to strengthen the domestic representative requirement for foreign businesses, expand rights (portability, automated-decision safeguards), and introduce stricter enforcement and supervisory obligations.



The amendments formalise additional duties for overseas entities (domestic representatives, increased disclosure) and include AI-related rules. Implementation timelines and enforcement specifics are being phased in - companies should update policies and appoint compliant domestic representatives if they process Korean personal data. **Read more** [here](#).

Saudi Arabia: PDPL Enforcement

Saudi Arabia's Personal Data Protection Law (PDPL) became enforceable in Sept 2024. Through 2025 the Kingdom progressed consultations and proposed amendments to its implementing regulations (SDAIA consultations), including expanded complaint timelines and clarifications on supervisory powers. Organisations processing Saudi personal data must meet PDPL obligations (lawful bases, cross-border protections, data subject rights) and monitor SDAIA/Sample implementing rules. **Read more** [here](#).



public-sector processing rules if enacted. **Read more** [here](#).

Babalakin and Co. is a licensed Data Protection Compliance Organisation.
If you have any questions or would like more information on the issues discussed, please contact: dataprivacy@babalakinandco.com



Olawale Adedipe

Associate
oadedipe@babalakinandco.com



Zainab Oladapo

Associate
zoladipo@babalakinandco.com



Afolabi Samuel Alawode

Trainee Associate
aalawode@babalakinandco.com

—OFFICE LOCATIONS—

LAGOS OFFICE

1261A Adeola Hopewell Street
Victoria Island, Lagos State.
(+234)2012718700, 2718806, 2718808,
2718711, 27188004, (+234)2702802

ABUJA OFFICE

4, River Benue Street,
Off Ibrahim Babangida Boulevard,
Maitama District, Abuja.
(+234) 9-2780930, 2780933-9

PORT HARCOURT OFFICE

3, Williams Jumbo Street,
Old GRA, Port Harcourt
Rivers State.
(+234)703506876