TERRALEX

Global Trends in Privacy and Data Protection 2026

2026 sees the tenth anniversary of the EU's approval of the General Data Protection Regulation. It's timely, then, that at the end of 2025, the European Commission published its proposals for reform of GDPR as part of its Digital Omnibus Regulation Proposal. Across the world, many other jurisdictions are looking to pass new laws in relation to privacy, data protection, and cyber as countries grapple with the legal and regulatory challenges posed by AI and other technology.

In this briefing, TerraLex experts from across the world pick out the key themes and developments for 2026.

Regulating artificial intelligence

Countries worldwide are increasingly aligning their efforts to strengthen AI oversight, with regulators sharpening their focus to ensure AI is developed and deployed responsibly.

Throughout 2025 and into 2026, we have seen several new laws being introduced to set robust standards for safe and transparent AI use, with an emphasis on protecting individual data rights.

Mirroring the approach of the EU AI Act, other jurisdictions are now adopting risk-based classification models that impose stricter requirements on higher-risk AI systems, recognising that the use of AI in certain contexts poses greater threat. To support effective implementation, regulators are also releasing practical guidance and playbooks designed to help organisations navigate compliance in real-world settings. Together, these developments reflect a rapidly evolving regulatory landscape aimed at embedding safety and accountability at the core of global AI governance.

However, there is also a recognition that law makers may not always get view the law right. The European Commission is proposing to review certain aspects of the EU AI Act.

In 2026, organisations that use automated decision-making technologies, including AI-driven tools, can expect increased regulatory scrutiny over how they collect and use personal data. Going forward, organisations will be required to demonstrate greater transparency and accountability in how they gather and process individuals' information. Understanding your global compliance obligations is essential.

Cyber risk

Global cyber security and privacy laws also continue to evolve, with many jurisdictions strengthening existing frameworks or introducing new ones over the course of 2026 to address emerging risks.

New and updated laws will increasingly require organisations to demonstrate proactive security measures, such as mandated cybersecurity audits and compliance with stricter notification of cyberattacks. Multinational organisations will need to ensure that they understand their obligations in different countries.

Facial recognition and biometric technology

Biometric data has become a major enforcement priority looking into 2026, with regulators in a number of countries cracking down on organisations who use facial recognition technology, without valid consent or robust security controls. Again, multinational businesses will need to ensure that they understand their compliance obligations in each country.

Children's data

The protection of children's data remains a clear priority as we move into 2026.

Across many jurisdictions, lawmakers are introducing new measures or strengthening existing frameworks to better safeguard children's information, particularly where social media and other digital services are concerned.

Regulators are particularly concerned with implementing stricter requirements for platforms accessible to children, by introducing age-verification processes and parental consent mechanisms and scrutinising how organisations

handle children's data. Other regulators are taking a more proactive approach, by investigating existing breaches involving children's data.

Although challenges remain, the direction of travel clearly demonstrates that there is a growing global commitment to creating safer online environments for children and holding organisations accountable when they fail to protect the most vulnerable users.

Key developments in Europe

In December 2025, the European Commission published its Digital Omnibus Regulation Proposal. The proposal sets out a package of measures intended to simplify compliance for businesses. This includes:

- amendments to the EU AI Act and delaying the coming into force of the rules applying to high-risk AI systems that were due to apply from August 2026
- simplifying cyber security reporting obligations
- amendments to the rules on cookies, and
- a number of targeted amendments to GDPR, including new rights for controllers to reject data subject access requests in certain circumstances and amendments o he definition of personal data.

Earlier in 2025, the UK approved a number of amendments to UK data protection law, which will increase the divergence between EU and UK data protection law post Brexit. The amendments, which will come into force in early 2026 will make it easier to use personal data in research (including potentially for AI training), reduce the regulation of automated decision making, and amend the rules on the transfers of personal data outside the UIK.

Turkey (a non-EU country) is aiming to align its data protection law with the GDPR by 2026.

As appears to be the theme into the new year, EU member states are focused on ensuring robust AI protection. While the EU AI Act continues to be rolled out in stages, there is a focus on providing effective AI governance on a country-level with Spain recently establishing the first dedicated AI regulator in Europe, known as the AESIA. Other countries have shown attempts to tackle AI head on, with the Higher Regional Court of Cologne in Germany recently permitting the use of data without consent for the purposes of training an AI model. The publication of practical guidance for the implementation of AI remains a popular tool across the board, with both Spain and Germany opting to introduce guidance or law to regulate its use.

Regulators in Poland are also scrutinizing the use of AI and biometric in employment and HR. Poland has also implemented new laws on electronic marketing, which include B2B marketing.

Cybersecurity looks to be a particular priority for Europe going into 2026. EU member states continue to implement the NIS 2 Directive (for example, Poland and Austria), but a several of member states are still to pass implementing legislation. Switzerland and Turkey are reforming or introducing cybersecurity laws which aim to broaden the regulatory scope to new sectors and focus on stricter notification of cyber incidents and extended powers for authorities.

The UK has also commenced the process for updating UK cyber security laws to expand the NIS Regulations to new sectors and entities. It is expected that the new laws will be approved in 2026. As with GDPR, this will create increasing divergence between EU and UK law for multinational organisations.

Other developments across Europe include the implementation of the EU Data Act (which sets out new rules for data sharing and reuse and came into force in September 2025), the introduction of electronic proof of identity in Switzerland to complement a physical passport which can be used to authenticate online ID, and the Electronic Health Register which has been rolled out in Germany subject to specific data protection requirements.

Key developments in the Americas

In the US, South America, and Canada, 2026 promises to be a year of tackling the most pressing data protection issues via enforcement action and the continued implementation of new and existing laws.

The US' primary focus centres around the practical implementation of data protection rules, particularly in connection with higher risk activities such as the use of AI, large-scale data sharing, and the use of children's personal data. This remains a patchwork of state level laws, with no federal privacy rules in sight. Key developments include new or amended laws in California, Colorado, Connecticut, Utah and New Jersey.

The spotlight continues to shine on AI regulation, with proposed state level laws based on a high-risk classification system and aims to harmonise state laws well underway via a National AI Policy Framework. As with other jurisdictions, the US looks to supplement legal action on AI with practical guidance, via its NIST Artificial Intelligence Risk Management Framework. The Children's Online Privacy Protection Act (COPPA) continues to be enforced in the US, though through a narrower lens. At a federal level, regulators are intensely scrutinising the use of children's data, whilst at a state level, new laws introducing age-verification and parental-consent requirements for online services accessible to children continue to emerge.

The US has also implemented new rules restricting bulk transfers of sensitive personal data and government-related data to "countries of concern". This imposes new compliance obligations on companies in relation to bulk transfers of data outside the US.

In Canada, regulators are increasingly active. In recent months, we have seen investigations by Canadian regulators against Tiktok in relation to a data breach involving children's personal data, and against OpenAI fin relation to the use of personal data without consent. In the background, the Canadian Government continues to consult on its national AI strategy and we await the introduction of a new bill setting out proposed changes to existing federal privacy legislation, including an update to PIPEDA.

In South America, new laws are expected on AI and data protection in both Brazil and Colombia. The Brazilian Data Protection Authority (ANPD) are making headway towards regulatory progress, with children's privacy and AI legislation on the agenda for the near future. Alongside proposals for new laws in relation to AI and data protection (including data portability and automated decision-making), Colombia's data protection authority has recently cracked down on the inadequate processing of sensitive data by ordering the shutdown of a company processing biometric data.

Key developments from other countries around the world

The continued theme of enhanced regulatory protection continues to echo through the rest of the globe. Elsewhere, such as in Saudia Arabia, we are seeing a move towards new laws to strengthen individuals' data and privacy rights, including a focus on regulating cross-border transfers.

Finally, in Australia, we are seeing a similar trend towards regulation of automated decision-making and children's privacy. From 10 December 2026, Australia will see both enhanced transparency requirements for automated decision-making and the introduction of a Children's Online Privacy Code to ensure robust protection for children's personal data in the online domain. The Australian Government is also expected to publish its proposals to update the Privacy Act 1988.

Summary

The laws on data, privacy and AI continue to evolve as governments and regulators try to keep up with evolving technology. Multinational organisations need to ensure that they keep up to date with the laws in each country in which they operate and understand how these laws impact on their global compliance programmes and use of technology.

If you would like to discuss how TerraLex member firms can help your organisation manage global compliance, please contact one of the contributing authors below or your local TerraLex member firm.

Contributors

Coordinated by Martin Sloan at Brodies LLP

Austria
Monica Sturm (monika.sturm@fwp.at)
Fellner Wratzfeld &Partners Rechtsanwälte (www.fwp.at)

Australia
Matthew McMillan (mmcmillan@landers.com.au)
Landers & Rogers (www.lander.com.au)

Brazil
Renata Ciampi (renata.ciampi@mottafernandes.com.br)
Motta Fernandes Advogados (www.mottafernandes.com.br)

Canada
Kristin Pennington (kristen.pennington@mcmillan.ca)
McMillan LLP (www.mcmillan.ca)

Colombia
Dario Cadena (dcadena@lloredacamacho.com)
Lloreda Camacho &Co (https://lloredacamacho.com/)

Germany
Krisina Schreiber (kristina.schreiber@loschelder.de)
Loschelder (www.loschelder.de)

Poland
Sabina Kubsik (kubsik@dt.com.pl)
Drzewiecki, Tomaszek i Wspólnicy Sp.j (www.dt.com.pl)

Saudi Arabia
James McMillan (james.mcmillan@erlf.com)
Eyad Reda Law Firm LLP

Spain
Beatriz Rodríguez Gómez (b.rodriguez@rocajunyent.com)
RocaJunyent (www.rocajunyent.com)

Switzerland
Cornelia Matig (cornelia.mattig@rfplegal.ch)
Roesle Frick & Partners (www.rfplegal.ch)

Turkey
Sevgi Ünsal Özden (sevgiunsal@erdem-erdem.com)
Erdem & Erdem Law Office (www.erdem-erdem.com)

United Kingdom
Martin Sloan (martin.sloan@brodies.com)
Brodies LLP (www.brodies.com)

USA
Amy Mushahwar (amushahwar@lowenstein.com)
Lowenstein Sandler (www.lowenstein.com)

Jenny Lewis Holmes (jholmes@nixonpeabody.com)
Nixon Peabody (www.nixonpeabody.com)

Global Trends in Privacy and Data Protection 2026

TERRALEX