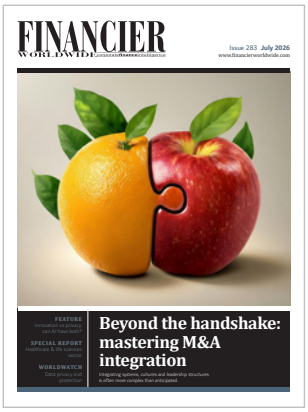

bahas gramatidis

This article first appeared in the July 2026 issue of Financier Worldwide magazine.

FINANCIER WORLDWIDE corporatefinanceintelligence

WORLDWATCH **REPRINT** July 2026

DATA PRIVACY AND PROTECTION

The criteria used to define personal data vary significantly across jurisdictions, legal contexts and technical standards. In some areas, the boundaries of personal data are being radically redefined, while in others the concept continues to be interpreted and enforced under existing legislation. As artificial intelligence systems continue to proliferate, organisations will require a robust and practical approach to data privacy and protection, grounded in operational readiness rather than reliance on paper-based compliance. ■

THE PANELLISTS

GREECE

POPI PAPANTONIOU
Counsel
Bahas, Gramatidis & Partners
T: +30 210 33 18170
E: p.papantoniou@bahagram.com

Popi Papantoniou heads Bahas, Gramatidis & Partners' data protection & digital law practice. With over 20 years of experience, she advises Greek and international clients on data protection, technology and AI law. Her expertise spans GDPR compliance, data governance, cyber security, AI regulation, e-commerce, digital platforms, cross-border data transfers and regulatory proceedings before supervisory authorities and courts.

ITALY

MATIA CAMPO
Partner
CMS Adonnino Ascoli & Cavasola Scamoni
T: +39 06 47815 1
E: matia.campo@cms-aacs.com

Matia Campo serves is partner in the technology, media and communications department. He assists national and international companies with respect to internet & media, telecommunications, e-commerce, regulatory and transnational matters, as well as in connection with complex outsourcing, SLA-based and IT agreements, artificial intelligence, robotics and data protection matters, advertising and unfair commercial practices. His experience includes assisting broadcasters and media companies in dealing with compliance and regulatory and media litigation and IT service agreements.

FRANCE

AHMED BALADI
Partner
Gibson, Dunn & Crutcher LLP
T: +33 (1) 5643 1300
E: abaladi@gibsondunn.com

Ahmed Baladi is a partner in the Paris office of Gibson Dunn. He is co-chair of the firm's privacy, cyber security and data innovation practice group, and a member of the artificial intelligence and technology transactions practice groups. He has developed renowned experience in a wide range of privacy matters, including the implementation of global privacy compliance and governance programmes tailored to complex and evolving regulations.

UNITED KINGDOM

LORE LEITNER
Partner
Gibson, Dunn & Crutcher LLP
T: +44 (0)20 7071 4987
E: lleitner@gibsondunn.com

Lore Leitner is a partner in the London and Brussels offices of Gibson Dunn and is a member of the privacy, cyber security and data innovation practice group. She has 15 years of experience advising clients on all aspects of tech law, including data protection and cyber security. During that time, she has guided several well-known technology companies through litigation and regulatory investigations, sometimes involving multiple agencies across the EU.

BELGIUM

BASTIAAN BRUYNDONCKX
Partner
Lydian
T: +32 (2) 787 9093
E: bastiaan.bruyndonckx@lydian.be

Bastiaan Bruyndonckx is a partner at Lydian, leading the technology and data practices. He specialises in data governance, cyber security, artificial intelligence (AI), IT regulation, technology contracting and e-commerce. He advises organisations across sectors on complex data and technology matters, including AI projects, GDPR compliance, digital regulation and large-scale ICT transactions. He is recognised by Legal 500 and Chambers Europe.

CANADA

CAEL HIBBERT
Associate
McCarthy Tetrault
T: +1 (604) 643 5969
E: chibbert@mccarthy.ca

Cael Hibbert is an associate in McCarthy Tétrault's Vancouver office and a member of the firm's national cyber/data and technology groups. His practice focuses on privacy and cyber security law. He advises clients on a broad range of privacy matters, including drafting and negotiating data processing agreements, preparing privacy policies and terms of use, conducting privacy impact assessments, advising on privacy considerations in technology and commercial agreements, and advising on artificial intelligence.

FW: HOW IS YOUR COUNTRY REDEFINING WHAT COUNTS AS PERSONAL DATA IN LIGHT OF AI-GENERATED OUTPUTS, BEHAVIOURAL PROFILES, AND BIOMETRIC OR NEURO DERIVED INFORMATION?

GREECE

Papantoniou: The doctrinal boundary of personal data in Greece is undergoing a radical redefinition under the profound impact of artificial intelligence (AI) systems. The Hellenic Data Protection Authority (HDPA) adopts an expansive, dynamic interpretation, whereby algorithmic outputs and behavioural profiling mechanisms are divested of their anonymous status insofar as they enable indirect identification, targeting or retrospective linkage to a natural person. Under the European Union (EU) AI Act, domestic regulatory focus is heavily concentrated on the strict prohibition of emotion recognition systems, particularly within workplace and educational environments. Commercial entities, such as data controllers, now confront a convergence of anonymous and protected information, as mere pseudonymisation is deemed insufficient to preclude the risk of reidentification. Consequently, generated data derived from algorithmic forecasting and neuro-derived insights constitute personal data, thereby mandating full regulatory compliance through compulsory data protection impact assessments (DPIA) under the General Data Protection Regulation (GDPR).

FRANCE

Baladi: Personal data is defined functionally under the GDPR recital 26, any element from which a person can be singled out by means reasonably likely to be used. In terms of AI, European Data Protection Board (EDPB) opinion 28/2024, endorsed by the French Data Protection Authority – CNIL – in its 2025 recommendations, confirms that a model falls within the GDPR wherever training data can be extracted, including through "regurgitation" in generative systems. Behavioural inferences are equally caught. In the 2023 *Schufa* case, the Court of Justice of the European Union (CJEU) held that an automated probability score constitutes a decision under article 22 of the GDPR "where a third party draws strongly on it" to determine a contractual outcome. Biometric data remains a special category under articles 4(14) and 9(1). The CNIL has since 2019 extended this to algorithmic outputs derived from raw biometrics where the original cannot be reconstituted. Neuro-derived data is the next frontier. Though not yet listed in article 9, the Council of Europe's T-PD committee published draft guidelines in 2025 applying Convention 108-plus principles to neural data.

CANADA

Hibbert: In Canada, the statutory definition of what counts as personal data has not formally changed. It is still "information about an identifiable individual", but regulators are applying it more expansively in practice. There is a shift away from focusing only on data that directly identifies someone, to also capturing inferred and derived information. Behavioural profiles, AI-generated outputs, biometric and neuro data, and similar data points can fall within scope where they can be linked back to an individual or used to make decisions about them.

BELGIUM

Bruyndonckx: Belgium does not redefine personal data through standalone national legislation, Rather, it applies the GDPR and the EU AI Act to emerging data types. The Belgian Data Protection Authority (BDPA) treats AI-generated inferences – such as behavioural profiles, scores and predictions – as personal data where they relate to an identifiable individual, even when derived from indirect signals such as browsing history or tone of voice. AI systems may also unlawfully infer sensitive attributes, including health status or sexual orientation, without the individual's knowledge

or consent. Biometric data, including behavioural biometrics, constitutes special-category data, the Constitutional Court confirmed in January 2025, in that facial recognition requires strict proportionality, explicit consent and immediate deletion after use. Neuro-derived data falls within the health or biometric categories. The BDPA takes the position that AI-derived scores cannot in themselves have probative value – meaningful human review is always required before any legally significant decision is taken.

UNITED KINGDOM

Leitner: The UK is slowly looking to move toward a more relative, contextual standard for personal data, where identifiability is assessed from the perspective of the particular party processing it, which means that information may be personal data for one actor but not another. The Data Use and Access Act and the Information Commissioner's Office (ICO) guidance both reflect this, though the legislator stopped short of broadening the definition in a way that might cost the UK its adequacy decision. The same trend is visible in the EU following the CJEU's recent *EDPS v SRB* judgment, which reintroduced a subjective standard for personal data so that data can be considered anonymous if held under certain conditions which prevent reidentification. This approach has the ability to reshape the treatment of AI-generated outputs and behavioural profiles. Biometric data sits differently – it is inherently or innately identifiable because its purpose and value lie in singling out a specific individual.

ITALY

Campo: Italy is not formally redefining the concept of personal data, but regulators are increasingly applying existing GDPR principles to technologies capable of generating, inferring or aggregating information about individuals in new ways. In practice, the Italian Data Protection Authority – Garante – tends to adopt a relatively broad interpretation whenever information may contribute – directly or indirectly – to the identification, profiling or singling out of a person. This approach is becoming particularly relevant in the context of AI-generated outputs, behavioural analytics, recommendation systems and advanced profiling tools. The regulatory focus is progressively shifting away from the technical format of the information toward the practical risk of reidentification or inference. This approach is broadly aligned with the direction of recent Italian AI legislation, which reflects growing regulatory attention toward transparency, accountability and the protection of individuals in AI-driven environments. Biometric data already benefits from enhanced protection under article 9 of the GDPR, and similar concerns are likely to emerge in relation to neuro-derived and other highly sensitive behavioural information as these technologies evolve further.

FW: FROM YOUR REGIONAL PERSPECTIVE, HOW HAS ENFORCEMENT CHANGED IN PRACTICE – PARTICULARLY IN TERMS OF AUDITS, PENALTIES, BREACH NOTIFICATIONS AND LITIGATION RISK?

FRANCE

Baladi: Enforcement in France has shifted from episodic to structured plans. The CNIL conducted 323 controls in 2025, triggered by complaints, breach notifications and ex-officio inspections. Sanctions have accelerated in parallel. In 2025 the CNIL issued 83 sanctions totalling almost €487m, with 67 routed through the fast-track procedure introduced in 2022, which allows fast-track fines. Breach notifications now function as an enforcement gateway – 6167 in 2025, around 10 percent year on year – and inadequate article 32 security remains a leading ground for enforcement. Cross-jurisdictional enforcement risk is rising in parallel. The CNIL adopted four sanctions in cooperation with EU regulators in 2025, and reviewed nine related European draft decisions affecting French residents.

CANADA

Hibbert: Enforcement in Canada is still less penalty-driven than in some jurisdictions, but it has become much more visible and practical in its impact. Regulators are more active, and investigations are increasingly coordinated across

federal and provincial authorities. Public reports play a significant role, and even without large fines the reputational impact can be similar. Breach notification is now a key trigger point. Organisations are expected to assess incidents against the 'real risk of significant harm' threshold and notify regulators and individuals where required, as well as maintain detailed internal records for all incidents. The bigger change is on the litigation side. Class actions now routinely follow high-profile breaches, which means organisations are managing regulatory exposure and litigation risk at the same time.

Class actions now routinely follow high-profile breaches, which means organisations are managing regulatory exposure and litigation risk at the same time.

CANADA CAEL HIBBERT
MCCARTHY TETRAULT

BELGIUM

Bruyndonckx: In Belgium, enforcement has shifted markedly from reactive complaint-handling to proactive, systemic scrutiny. The BDPA's Inspection Service opened 157 new dossiers in 2024 – an 83 percent increase compared to 2023 – with AI systems, data brokers and cookie banners as key priorities. Breach notifications reached 1455 in 2024, up 13 percent year on year, with ransomware attacks under active investigation. The BDPA has adopted an increasingly assertive posture. It now routinely sends follow-up questions to controllers, notably requesting details on the methodology used to assess the risk level of a breach. Breach notifications can trigger formal proceedings before the Litigation Chamber, particularly where the controller lacked adequate processes to handle data subject rights requests or maintained insufficient technical and organisational measures. On penalties, Belgium remains relatively conservative – total fines imposed in 2024 reached €708,371, with individual sanctions including a €174,640 fine against a data broker and a €250,000 fine against IAB Europe. Litigation risk is material and growing, with 10 appeals lodged before the Brussels Market Court in 2024, and six decisions partially or wholly annulled. Critically, the Market Court has confirmed that a single incident can trigger a full GDPR audit of an entire organisation, a development that practitioners must take seriously.

UNITED KINGDOM

Leitner: Enforcement has fundamentally changed in character. In the early days of the GDPR, the ICO acted largely alone. Today it operates within a dense web of overlapping regimes, the Online Safety Act, the Network and Information Security Directive 2 (NIS2), and emerging AI regulation, alongside regulators like Ofcom and the Competition and Markets Authority, each with its own notification triggers and audit powers. A single incident or compliance failure can now expose a business to parallel investigations, breach notifications on differing timelines, and cumulative penalties across authorities. Litigation risk has become multidimensional – the real challenge is mapping how regulators interact and anticipating where they are heading, rather than satisfying any one of them. It is one of the things that keeps the work both challenging and interesting.

ITALY

Campo: Privacy enforcement in Italy has become significantly more

operational and technically focused over the last few years. Regulatory investigations increasingly go beyond formal documentation and examine how organisations manage cyber security measures, internal governance, vendor oversight and incident response processes in practice. The Garante has been particularly active in areas such as telemarketing, unlawful profiling activities, inadequate security measures and insufficient accountability frameworks. At the same time, scrutiny around breach notifications has increased, especially where incidents are reported late or internal escalation procedures appear ineffective. Recent CJEU case law confirming the availability of compensation for non-material damages under the GDPR has also increased organisational focus on potential litigation exposure. From a practical standpoint, many organisations now view privacy compliance less as a purely legal exercise and more as part of a broader governance and risk management function.

GREECE

Papantoniou: Data protection enforcement in Greece has shifted from simple recommendations to strict, deterrence-focused action. The HDPA actively conducts extensive ex-officio audits, targeting illegal direct marketing and major security breaches. This trend is clear from landmark rulings, such as the Ministry of Interior being fined €400,000 after an electoral data leak, and the imposition of a historic €2.9m penalty on Hellenic Post for weak cyber security following a ransomware attack. Recent sanctions also highlight this focus, including an €80,000 fine for bypassing the national advertising opt-out registry and a €30,000 fine for violating data subject rights. Concurrently, civil litigation risk is rising sharply. Affected individuals increasingly file lawsuits under article 82 of the GDPR in conjunction with articles 299 and 932 of the Greek Civil Code, to claim compensation for non-material damages, such as moral distress, with Greek courts steadily awarding €1000 to €5000 per data subject.

Privacy and cyber security regimes are converging rapidly. NIS2 and DORA go significantly further than GDPR alone.

BELGIUM BASTIAAN BRUYNDONCKX
LYDIAN

FW: DO YOU SEE THE GLOBAL FRAMEWORK FOR CROSS-BORDER DATA TRANSFERS BECOMING PERMANENTLY FRAGMENTED? HOW ARE ORGANISATIONS IN YOUR COUNTRY ADAPTING TO LOCALISATION AND VENDOR CHAIN RISK?

CANADA

Hibbert: Canada's privacy framework can seem fragmented, but the approach remains practical. Cross-border data transfers are still generally allowed, and organisations are expected to understand and manage the risks involved. In practice, the focus has shifted to vendor and supply chain oversight. It is no longer enough to diligence the primary vendor. Organisations need visibility into subcontractors, data flows and access across the chain. We are seeing more detailed contractual protections, audit rights and security requirements. Some organisations are looking at keeping higher-risk data in Canada, but

many are keeping cross-border transfers and focusing on managing the risks.

BELGIUM

Bruyndonckx: The global framework for cross-border data transfers remains permanently fragmented, and no convergence is foreseeable in the near term. Ongoing uncertainty surrounding the EU-US Data Privacy Framework compounds this fragmentation. In practice, large organisations have responded by layering multiple safeguards simultaneously – relying on the EU-US Data Privacy Framework for certain categories of data while deploying binding corporate rules or standard contractual clauses (SCCs) for others, depending on the sensitivity of the transfers and the nature of the data involved. Vendor chain risk management is no longer a GDPR-exclusive concern. Organisations are increasingly integrating their data transfer due diligence into a broader compliance framework encompassing NIS2 and the Digital Operational Resilience Act (DORA), both of which impose their own third party and supply chain risk obligations. The result is a layered regime in which GDPR transfer assessments sit alongside – and must be reconciled with – cyber security-driven vendor management requirements, significantly increasing the compliance burden across the entire supply chain.

A single incident or compliance failure can now expose a business to parallel investigations, breach notifications on differing timelines, and cumulative penalties across authorities.

UNITED KINGDOM LORE LEITNER
GIBSON, DUNN & CRUTCHER LLP

UNITED KINGDOM

Leitner: I do not see permanent fragmentation as a challenging status quo, but instead see clients settling into a more complex but workable equilibrium. Cross-border transfers were heavily litigated around the time of the Schrems cases, but most organisations have matured past the panic stage, building durable frameworks into business as usual. This extends beyond the EU, to localisation pressures and access regimes worldwide, including compliance with US instruments like the Committee on Foreign Investment in the United States and the recent bulk sensitive data rules. What I would stress is that legal compliance and vendor chain risk are not the same thing. Securing supply chain needs a different toolkit – robust contractual protections and flow-downs, onboarding due diligence repeated through the relationship rather than as a tick-box, audit rights and a demonstrably current security programme. The organisations that manage this well treat transfers, localisation and vendor risk as one connected problem, not three separate silos.

GREECE

Papantoniou: Global fragmentation in cross-border data transfers is becoming permanent due to geopolitical tensions. In Greece, businesses rely heavily on international cloud providers, making transfers to the US a major focus. Despite the EU-US Data Privacy Framework, the fear that courts might cancel this agreement again forces Greek organisations to manage vendor chain risk strictly. They closely follow the HDPA's Guidelines 4/2023 on cloud computing. In practice, companies require the systematic use of SCCs,

strict TIAs and a clear shift toward storing data within the EU. Checking subprocessors is now a core part of commercial contracts. Greek companies fully realise that under the GDPR, the final responsibility for any compliance failure in the supply chain belongs to them as data controllers.

ITALY

Campo: Many Italian organisations increasingly assume that uncertainty around international data transfers is likely to remain a structural feature of the regulatory landscape. While mechanisms such as SCCs and the EU-US Data Privacy Framework continue to provide workable legal solutions, companies generally no longer consider transfer compliance a one-time contractual exercise. In practice, organisations are dedicating greater attention to vendor assessments, data flow mapping, cyber security safeguards and transfer impact evaluations, particularly where non-EU cloud providers are involved. This trend is especially visible in regulated sectors and in projects involving critical infrastructure, financial services, healthcare or public-sector data. At the same time, there is growing interest in EU-based hosting solutions and sovereign cloud models, partly driven by cyber security concerns and partly by broader governance and operational resilience considerations. For many Italian companies, the most difficult challenge is not understanding the legal rules themselves, but ensuring consistent coordination between legal, procurement, IT and cyber security functions across increasingly complex international supply chains.

The practical priority is documented governance – tested incident-response, mapped vendor chains and board-level cyber and AI risk minutes.

FRANCE AHMED BALADI
GIBSON DUNN

FRANCE

Baladi: Cross-border data transfers under the GDPR rest on a layered framework. Adequacy decisions, SCCs and other chapter 5 mechanisms govern the general conditions for transfer, while article 49 provides limited derogations and article 48 addresses the specific scenario where foreign courts or public authorities order disclosure of personal data without an applicable international agreement. The core tension exposed by Schrems II sits precisely at this intersection. The 2023 EU-US Data Privacy Framework attempted to resolve this through Executive Order 14086, but its adequacy decision faces an ongoing CJEU appeal, leaving residual uncertainty about the durability of any transatlantic transfer mechanism. France has responded within a clear digital sovereignty doctrine. Article 31 of the 2024 Sécurité et Régulation de l'Espace Numérique law requires that sensitive public sector data be hosted exclusively by providers holding ANSSI's SecNumCloud 3.2 qualification, a standard that structurally excludes providers subject to extraterritorial foreign laws, precisely the scenario article 48 is designed to guard against. Private-sector organisations are applying parallel logic: EU-based hosting, end to end encryption, rigorous article 28 GDPR vendor due diligence and Schrems II TIAs as part of their broader chapter 5 compliance.

FW: HOW ARE PRIVACY AND DATA PROTECTION REGIMES INCREASINGLY TYING CYBER SECURITY RESILIENCE, INCIDENT RESPONSE AND BOARD-LEVEL ACCOUNTABILITY TOGETHER? WHAT DOES THIS MEAN IN PRACTICE FOR SENIOR LEADERSHIP WHEN THINGS GO WRONG?

Italian organisations should increasingly approach privacy and cyber security compliance as part of a unified governance strategy rather than as isolated regulatory workstreams.

ITALY MATIA CAMPO
CMS ADONNINO ASCOLI & CAVASOLA SCAMONI

ITALY

Campo: In Italy, privacy compliance is increasingly converging with cyber security governance and operational resilience requirements. The combined effect of the GDPR, the NIS2 framework and sector-specific rules such as DORA is pushing organisations toward a more integrated approach to risk management and internal accountability. Regulators now expect senior management and boards to play a more active role in supervising cyber security and data protection issues, rather than treating them as matters handled exclusively by technical teams. In practical terms, this means approving risk management measures, overseeing incident response procedures, and ensuring that reporting and escalation mechanisms function effectively. The operational pressure on organisations has increased significantly because a single cyber incident may trigger multiple obligations simultaneously, including GDPR breach notifications, cyber security reporting duties, contractual obligations toward customers and, potentially, criminal law implications in more serious cases. Many Italian organisations are still adapting to this shift, particularly where privacy, compliance and cyber security functions historically operated in separate silos.

UNITED KINGDOM

Leitner: Cyber resilience regimes are rewriting who is accountable when security fails. The GDPR historically required security appropriate to risk, but largely treated this as an organisational obligation. New cyber resilience rules go further, making resilience, incident response and senior accountability explicit and auditable. In some cases, management bodies must approve and oversee security measures, undergo training and face personal liability where they fail. This changes what gets scrutinised when things go wrong. Regulators no longer ask only whether an organisation was breached, but whether its leadership understood the risk, resourced it and governed it. Questions are retrospective and often uncomfortable. Did the board act on risk reporting? Was there a tested incident response plan? Was security adequately funded? A board that can produce minutes, training records and tabletop results is in a far stronger position than one that cannot. The upside of convergence in cyber-related laws is that one well-governed framework can satisfy multiple regimes at once. Organisations doing this well treat these obligations as part of a single governance architecture, not parallel compliance tracks.

FRANCE

Baladi: Privacy and cyber resilience are now structurally integrated. The GDPR ties

processing to "appropriate technical and organisational measures" and requires notification of breaches to the CNIL within 72 hours. The NIS2 adds an early warning to competent authorities – the French Cybersecurity Agency – within 24 hours, full notification within 72 hours and a final report within one month. The DORA tightens this further for financial entities, requiring major information and communications technology (ICT) incident reports within four hours of classification. The most consequential shift for senior leadership is the NIS2's article 20 – management bodies must formally approve cyber security measures and can be held personally liable for infringements. For essential entities, article 32(5) goes further, as national authorities may temporarily prohibit chief executives or legal representatives from exercising managerial functions for persistent non-compliance, not merely following a breach. The 2025 Digital Omnibus proposal aims to streamline these overlapping regimes into a single notification channel, though it remains subject to legislative adoption.

GREECE

Papantoniou: In Greece, cyber security resilience is directly tied to board-level accountability under Law 5160/2024, which implements NIS2. Supervised by the National Cybersecurity Authority (NCSA), this framework extends mandatory compliance to thousands of medium and large companies across critical sectors, including healthcare, energy, transport, logistics and digital services. In practice, senior executives face immediate legal exposure. Board members must personally approve cyber security measures and oversee incident response – they can no longer plead ignorance. When a major breach occurs, management faces severe personal consequences, including administrative sanctions and civil liability. Even for companies outside the scope of NIS2, the GDPR's accountability principle requires directors to ensure a robust security infrastructure through appropriate technical and organisational measures. Ultimately, regulatory authorities closely examine board decisions whenever security failures impact the supply chain.

BELGIUM

Bruyndonckx: Privacy and cyber security regimes are converging rapidly. NIS2 and DORA go significantly further than GDPR alone – DORA explicitly requires a designated board-level member responsible for ICT risk management, while NIS2 provides that natural persons representing essential entities may be held personally liable for failure to comply, for example where management bodies fail to approve and oversee cyber security risk measures. Regulatory scrutiny now extends beyond whether appropriate policies existed on paper. Regulators will examine whether senior leaders were adequately trained and whether they responded appropriately when incidents occurred. Given the breadth of applicable legislation – GDPR, DORA, NIS2 and the Cyber Resilience Act – board members

Board members must personally approve cyber security measures and oversee incident response – they can no longer plead ignorance.

GREECE POPI PAPANTONIOU
BAHAS, GRAMATIDIS & PARTNERS

can no longer approach these frameworks in silos. A transversal approach is essential. The GDPR must be understood in the context of the broader regulatory ecosystem. Personal accountability at board level is now an enforceable reality. When data protection officer (DPO) advice is disregarded and security measures prove inadequate, leadership cannot shelter behind organisational complexity. Documenting governance decisions, heeding DPO recommendations and conducting genuine DPIAs are now board-level risk management imperatives.

CANADA

Hibbert: In Canada, privacy compliance is increasingly assessed through cyber readiness and incident response. When something goes wrong, regulators and courts look closely at what was in place before the incident, how it was handled and what steps were taken after. In practice, organisations are expected to have a clear incident response plan, know who needs to be involved and keep good records throughout. For leadership, the key is to show they acted responsibly at every stage, rather than to prove the incident could have been prevented entirely.

FW: LOOKING AHEAD, WHAT PRACTICAL STEPS SHOULD ORGANISATIONS IN YOUR COUNTRY PRIORITISE NOW TO STAY AHEAD OF REGULATORY AND ENFORCEMENT TRENDS?

BELGIUM

Bruyndonckx: First, a genuinely transversal compliance approach is essential. The GDPR must be read alongside NIS2, DORA and the Cyber Resilience Act, not in isolation. Risk assessments, vendor due diligence, incident response and board governance must be aligned across all applicable regimes simultaneously. Organisations that continue to treat these frameworks in silos will find themselves structurally underprepared when enforcement action materialises. Second, board-level upskilling is no longer optional. Given the personal accountability provisions under NIS2 and DORA, ensuring that board members receive adequate training on cyber security risks is now an enforceable regulatory expectation, not merely a governance best practice. Third, organisations must critically revisit their 2018 GDPR implementation. Many compliance frameworks established when the GDPR entered into force have not kept pace with subsequent regulatory developments. GDPR compliance is not a one-time exercise – documentation, procedures and risk assessments require continuous review and updating.

UNITED KINGDOM

Leitner: To futureproof regulatory compliance, my main advice is to stop running parallel compliance tracks and build one integrated governance architecture with accountability at various levels of the organisation, including senior levels. These should be evidenced in advance, with the ability to flex across multiple regimes. Practically, I would prioritise four things. First – whether a platform, a hardware manufacturer or a retail-tech business – a full regulatory perimeter should be mapped, as organisations answer to several regulators at once, and overlaps between data protection, online safety, and product and competition rules are where exposure could arise. Second, get ahead of new legal regimes, make sure policies and procedures are reviewed and updated, including mapping and other documentation efforts like risk assessment, and review automated-decision-making practices rather than running on pre-2025 assumptions. Third, govern data and AI use deliberately – know what is held, why and on what lawful basis, as regulators scrutinise profiling, connected devices and AI more closely. Fourth, build genuine demonstrability, because regulators increasingly ask not whether the organisation complied, but whether it can show it. The organisations that fare best will evidence good governance, not perfection.

FRANCE

Baladi: Organisations should plan for three converging fronts. First, enforcement intensity will not abate. The CNIL issued 83 sanctions totalling €486.8m in 2025, with cookies, employee monitoring and article 32 security as the dominant grounds. Its 2025-28 strategic plan

sets four priorities – AI, protection of minors, cyber security and mobile applications and digital identity – and its 2025 thematic controls notably target mobile apps and software development kit permissions, and the right to erasure in a coordinated European action. Second, AI Act compliance becomes binding. Annex III high-risk obligations apply from 2 August 2026 and product-track from 2 August 2027, with the CNIL positioning itself as French market surveillance authority for fundamental-rights systems. Third, cyber governance accountability hardens. The NIS2's pending French transposition – *loi Résilience* – will extend director liability to roughly 15,000 entities, while DORA already vests ultimate ICT-risk responsibility in the management body. The practical priority is documented governance – tested incident-response, mapped vendor chains and board-level cyber and AI risk minutes.

GREECE

Papantoniou: To stay ahead of tightening regulatory trends, Greek organisations must transition from fragmented compliance to an integrated data governance framework. First, they should unify their GDPR, NIS2 and AI Act strategies by establishing a joint oversight structure where the DPO, chief information security officer and legal departments collaborate closely, giving the board unified visibility into digital risks. Second, companies must prioritise continuous supply chain auditing. Simply signing standard contracts is no longer enough; performing proactive vendor risk assessments and verifying subprocessors is vital. Finally, leadership must invest in practical staff training and incident simulation exercises. Regulatory enforcement by authorities like the HDPA and the NCSA focuses on operational readiness rather than paper-based compliance. By building a robust internal security culture, organisations safeguard their reputation and shield management from personal liability.

CANADA

Hibbert: Many organisations do not need to reinvent their privacy programmes. The focus is on making sure they work in practice and can hold up if tested. The key priorities are having a clear and tested response plan, knowing what data they hold and where it sits, and putting stronger contractual protections in place with third parties. Organisations that do this well are not building their response from scratch during an incident. They are following a plan they have already tested, which is what regulators and courts tend to focus on in practice.

ITALY

Campo: Italian organisations should increasingly approach privacy and cyber security compliance as part of a unified governance strategy rather than as isolated regulatory workstreams. Regulators are paying closer attention not only to formal documentation, but also to whether governance processes are genuinely operational and embedded in day to day activities. From a practical perspective, organisations should prioritise stronger coordination between legal, compliance, IT, procurement and cyber security teams, particularly in relation to incident management, vendor oversight and international data transfers. Vendor contracts and cloud arrangements should be reviewed regularly to ensure that legal, technical and operational safeguards remain aligned. Companies deploying AI systems should also assess transparency, profiling and human oversight issues carefully, especially where automated decision-making tools may affect individuals directly. More broadly, Italian organisations are discovering that effective compliance increasingly depends on governance maturity, internal coordination and the ability to demonstrate accountability in practice rather than solely through formal policies. ■