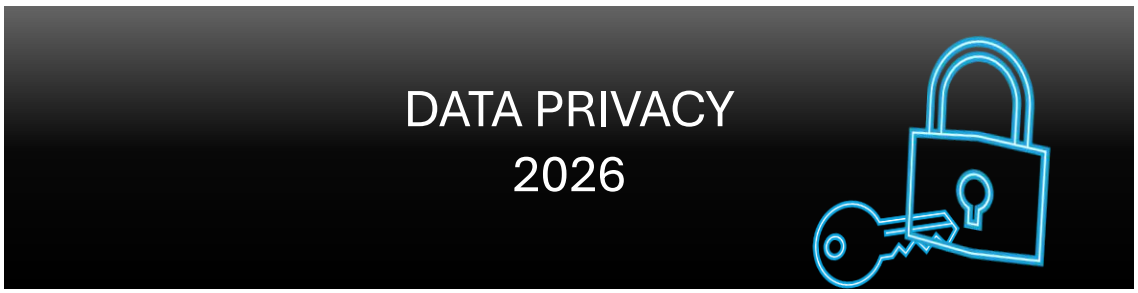
20th of January 2026



by **Nikoletta Maouri**, Legal & Compliance Director - geevo®

Privacy Day

Data Privacy Day is observed each year on January 28th, marking the signing of Convention 108 in 1981, the first legally binding international treaty dedicated to protecting privacy and personal data. While its roots are historical, the day serves as a reminder of the critical importance of privacy in today's rapidly evolving digital world.

This year, Data Protection Day 2026, is jointly organised by the Council of Europe (CoE) and the European Data Protection Supervisor (EDPS) and aims to explore the challenges and opportunities that arise when innovation and emerging technologies intersect with privacy risks and the regulatory frameworks, so the question is "*Reset or Refine*"?

GDPR: More than a Regulation

The General Data Protection Regulation (GDPR) represents more than a regulatory framework and a set of rules; it forms the foundation of the European Union's digital rulebook. Its territorial scope extends beyond the borders of the European Union, applying not only to organizations established within the EU, but also to those outside the EU that process personal data of individuals located in the Union, particularly where goods or services are offered or behavior is monitored.

Since its implementation, the General Data Protection Regulation has played a central role in shaping global approaches to data protection and privacy governance. Its extraterritorial reach and strong enforcement mechanisms have influenced legislation far beyond the European Union. Nevertheless, the effectiveness of the GDPR in addressing contemporary data-processing realities has become the subject of increasing academic and regulatory debate.

Privacy Challenges in the Digital Era

Technological innovation has reshaped personal data processing at an unprecedented scale. Artificial intelligence systems, large-scale analytics, and interconnected digital devices operate through continuous data flows that challenge traditional regulatory assumptions. In response, the European Union has developed a layered digital regulatory framework, including the AI Act, DMA, DSA, DORA, the e-Privacy Directive, and the NIS2 Directive, aimed at strengthening digital governance and risk management.

Despite this expanding legislative landscape, GDPR remains the central pillar of EU data protection law. Its principles of lawfulness, fairness, transparency, and accountability continue

to underpin the Union's digital strategy. Nevertheless, the practical application of these principles has become increasingly complex as automated decision-making, profiling, and real-time data processing blur conventional boundaries of control and responsibility.

Effective data protection can no longer be assessed solely through the existence of written policies. Rather, it depends on how compliance obligations are operationalised within organizational structures, technical systems, and decision-making processes. This includes continuous risk assessment, internal accountability mechanisms, and demonstrable compliance aligned with regulatory expectations.

Accordingly, modern data governance increasingly prioritizes outcome-based compliance. Innovation is expected to coexist with privacy protections through enforceable safeguards that are embedded within business operations, rather than treated as supplementary legal obligations.

A proactive approach to Privacy

Many organizations continue to approach privacy in a reactive manner, responding only after data breaches, customer complaints, or regulatory investigations have occurred. This approach often leads to increased financial penalties, reputational damage, and loss of stakeholder trust. In contrast, implementing robust and well-designed privacy controls at an early stage significantly reduces the likelihood of such incidents, while also demonstrating a genuine and sustained commitment to protecting personal information.

A proactive privacy strategy requires embedding data protection principles into everyday business operations, decision-making processes, and system design. This includes adopting practices such as privacy by design and by default, conducting regular data protection impact assessments, maintaining accurate data inventories, and ensuring that employees receive ongoing privacy training. By anticipating risks rather than merely reacting to them, organizations are better positioned to identify vulnerabilities before they escalate into serious compliance failures.

Privacy should therefore be viewed as an ongoing strategic investment rather than a one-time compliance exercise. Although establishing effective privacy governance frameworks may require upfront financial and operational resources, the long-term benefits are substantial. These include stronger organizational resilience, enhanced corporate reputation, improved customer confidence, and greater adaptability to evolving regulatory requirements. Ultimately, organizations that prioritize proactive privacy management are more likely to achieve sustainable compliance while fostering long-term trust in an increasingly data-driven digital environment.

Building a Practical Data Privacy Roadmap

A structured privacy roadmap is essential for moving from reactive compliance to operational maturity.

In establishing a strong roadmap, organizations need to:

- **Embed legal obligations into everyday work practices** – make sure regulatory requirements are reflected in operational practices.
- **Apply risk-based controls** – direct resources to areas where personal data is most vulnerable.
- **Combine privacy and cybersecurity strategies within broader governance frameworks** – integrate privacy considerations into broader IT and risk governance.

- **Assign clear responsibilities** – designate accountability for privacy tasks and oversight.
- **Commit to continuous enhancement** – treat privacy management as a continuous, evolving effort rather than a static checklist.

Controls and Security Systems as the Foundation

Effective privacy compliance depends on strong technical and organisational controls.

Regulators increasingly expect organisations to implement measures appropriate to the sensitivity and risk level.

Key areas include:

- **Data governance:** ownership, data mapping, classification, retention, and secure deletion
- **Access and identity management**: role-based access, least-privilege principles, and monitoring of privileged accounts
- **Information security**: encryption, endpoint protection, secure configurations, and network security
- **Incident response and breach management**: tested response plans and regulatory notification procedures
- **Third-party risk management**: vendor due diligence, contractual safeguards, and ongoing monitoring
- **Ongoing assurance**: audits, control testing, and measurable compliance indicators

Together, these controls form the operational backbone of a mature and effective privacy programme.

Looking Ahead

Data privacy must be recognised as a strategic asset rather than a regulatory burden. By embedding privacy into governance structures, technical controls, and everyday decision-making, organizations can transform compliance into resilience and trust. The future of the

GDPR does not lie in a fundamental reset, but in thoughtful refinement — one that enhances clarity, strengthens accountability, and ensures practical applicability in an increasingly complex digital environment. In doing so, privacy becomes not only a mechanism for protecting individual rights, but a cornerstone of sustainable innovation and long-term competitive advantage.

GDPR does not need a reset, it needs refinement through clarity, accountability, and operational enforcement.

Data privacy is not merely a regulatory obligation, but a foundational element of security, trust, and long-term competitive advantage!