Digital Society and Data Protection (summary)

Kazuki SHISHIDO

Partner, Uryu & Itoga

This paper provides an overview of the rapid evolution of personal data protection and privacy laws worldwide, driven by the advancement of the digital society. The implementation of the EU General Data Protection Regulation (GDPR) in 2018 has served as a catalyst for legislative reforms and new data protection frameworks across many jurisdictions. While some degree of harmonisation has been sought, countries have also introduced unique regulatory requirements, such as data localisation obligations and strict cross-border data transfer rules, reflecting their own economic, social, and security needs.

In the United States, comprehensive privacy laws have been enacted at the state level, such as the California Consumer Privacy Act (CCPA), while the EU has introduced the AI Act to regulate artificial intelligence systems based on risk. China and Russia have established stringent state-led data management regimes, including mandatory data localisation and broad governmental access to data. Countries such as India and Indonesia are also transitioning from fragmented sectoral rules to comprehensive frameworks inspired by the GDPR but incorporating local elements, such as the establishment of a Data Protection Board in India to oversee compliance and consent management.

Common elements among these laws include the definition of personal data, special regulations for sensitive data, the distinction between controllers and processors, legal bases for data processing (such as consent or legitimate interests), cross-border transfer restrictions, data subject rights, data localisation requirements, and severe administrative sanctions for violations. However, there are significant differences in the scope, enforcement, and practical operation of these laws, resulting in a complex and diverse global regulatory landscape.

For multinational enterprises, compliance challenges have intensified due to the extraterritorial application of data protection laws, exposure to substantial fines, and requirements for local language documentation and the appointment of local representatives. In global consumer product launches and e-commerce operations, companies must prepare tailored privacy policies, obtain consent in accordance with local law, and address cross-border transfer restrictions, making unified UI/UX design difficult.

As data is increasingly regarded as a national asset, many countries are strengthening data localisation obligations and restricting cross-border flows, raising the need to balance data protection with the free flow of information. The so-called “Brussels Effect”, whereby EU data protection standards become *de facto* global norms, is increasingly evident, especially with the adoption of the AI Act. Businesses must closely monitor these developments and adopt a risk-based approach to compliance in order to navigate the evolving global data governance landscape.