

April 2, 2025

THE EU DATA ACT: KEY TAKEAWAYS AND STRATEGIC RESPONSES FOR GLOBAL COMPANIES

I. BACKGROUND AND PURPOSE

The European Union (the “EU”) enacted the Data Act (Regulation (EU) 2023/2854) (the “**Data Act**”) as part of its European Strategy for Data, aiming to revitalize the data economy and promote digital transformation. The Act will be implemented in stages starting from September 12, 2025, following a grace period of approximately 20 months.

In light of the growing economic value and importance of data—driven by the proliferation of the Internet of Things (IoT) and connected products—the Data Act seeks to establish a data sharing ecosystem. It aims to prevent monopolies by dominant companies and promote fair access to and use of data, thereby addressing issues of market imbalance and data concentration.

II. MAIN CONTENTS OF THE DATA ACT

1. Scope

- The Data Act applies to data generated through the use of connected products and related services in the EU. It covers both personal and non-personal data held by business operators. Raw or pre-processed data is included, while inferred or derived data and content are excluded.
- A “connected product” is defined as a product that can obtain, generate or collect data concerning its use or environment, and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user. This includes both consumer and industrial products, such as connected cars, health monitoring devices, smart home devices, smartphones, and industrial or agricultural machinery.

2. Entities subject to the Data Act include manufacturers of connected products placed on the EU market, related service providers, users (both individuals and legal entities), data holders, data recipients, public sector bodies and data processing service providers. Obligations of Connected Product Manufacturers and Related Service Providers

- Manufacturers and related service providers must design, manufacture, and provide connected products and related services in a way that allow users to access the data easily, securely, and free of charge.

- Prior to entering into a product sales/rental agreement or a service contract, manufacturers and related service providers must inform users, clearly and understandably, about the types of data generated, the data retention period, how users can access, retrieve, and delete data, and any potential third-party use of the data.

3. User Right to Access Data

- If a user lacks direct access to their data, the data holder must provide it without delay, in a comprehensive, structured, commonly used and machine-readable format, with quality equivalent to what the holder retains.
- However, a user's right to access data may be limited in cases where such processing would undermine the security requirements of the connected product and have a seriously adverse impact on the health or safety of natural persons, or where the disclosure of trade secrets is highly likely to cause serious economic damage to the data holder. Access rights may be restricted if providing the data compromises product security, endangers health or safety, or risks serious economic harm through the exposure of trade secrets.

4. Right to Request Data Sharing by Users of Connected Products and Related Services

- Users have the right to request that the data holder provide the product and service data, along with the relevant metadata necessary to interpret and utilize such data to third parties.
- Data holders must ensure interoperability to facilitate seamless data transfer and minimize technical barriers. They must also provide the necessary technical and administrative support necessary. However, this right does not extend to data generated during testing of new connected products or procedures yet to be released to the market (unless the use of such data by third parties is permitted under the agreement).

5. Ensuring Transition Between Data Processing Services

- Providers of data processing services (such as cloud, edge computing, network, servers and other physical or virtual infrastructure and software) must implement technical measures to ensure that users can seamlessly transition between data processing services without loss of data or functionality.
- Until January 12, 2027, the data processing service provider may charge the actual costs incurred, but thereafter is prohibited from charging any costs related to the transition of services.

6. Ensuring Fairness in Inter-Company Data Agreements

- Data access and use agreements must be fair and transparent. Contractual terms that disadvantage one party -- such as excluding or limiting liability for willful or gross negligence, or excluding remedies or liability for failure to perform the agreement—are prohibited and deemed null and void.

- The European Commission plans to develop model contractual terms in connection with access/use of data to assist parties in negotiating fair agreements.

7. Use of Public Sector Data

- Public agencies may request data from private data holders only in exceptional situations, such as emergencies or for public services.
- They must justify the purpose and need for data request, and limit it to the minimum necessary. Data holders must respond without delay upon a legitimate request from a public agency, such as in an emergency, but must comply with strict conditions to protect security and trade secrets.

III. RELATIONSHIP BETWEEN DATA ACT AND GDPR

- Whilst both the Data Act and the EU's General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**") regulate data, the GDPR focuses on transparency in the processing of personal data and protection of data subjects' rights, whereas the Data Act aims to promote fair access/use of personal data and non-personal data from connected products and related services.
- The Data Act and the GDPR are complementary. However, where personal data is involved, the GDPR and the relevant national laws take precedence. Therefore, stakeholders must still comply with the legal requirements set forth in the GDPR when processing personal data.

IV. SIGNIFICANCE AND IMPLICATIONS OF THE DATA ACT

- **[Democratizing Data and Strengthening Users' Rights]** The Data Act seeks to democratize the data economy by mitigating data monopoly and strengthening users' data sovereignty through improved data access and mobility. Users gain greater autonomy over their data and can more easily shift between platforms.
- **[Standardization of Global Data Regulations]** While the existing laws on data are mainly focused on personal data, the Data Act addresses non-personal data. It is likely to influence data regulations in other countries. Therefore, global companies are advised to pay attention to data-related legislation in other countries and reassess their data management and contractual procedures in light of the balance between EU regulations and regulations in other countries.

V. CONCLUSION

The Data Act marks a significant step toward fairness and transparency in the data economy. It is expected to have substantial implications for global companies, especially those providing connected products and services to the EU market, as they will be required to establish systems to support user data access and portability, thereby necessitating changes in data processing practices.

Each EU member state must establish penalties for non-compliance with the Data Act and notify the European Commission by September 12, 2025. Companies must monitor legislative developments across the EU and ensure compliance with both the Data Act and the GDPR. A comprehensive, multi-faceted strategy is essential, including updates to technical systems and contractual terms for data-sharing.

BKL will continue to monitor changes in domestic and overseas regulations related to the Data Act and offer tailored advice to meet client needs in response to this evolving legal landscape.

Related Professionals

Jiyoung Sohn

Senior Foreign Attorney (New York)

T 82.2.3404.0241

E jiyoung.sohn@bkl.co.kr

Juho Yoon

Partner

T 82.2.3404.6542

E juho.yoon@bkl.co.kr

Jeonghee Kang

Partner

T 82.2.3404.6480

E jeonghee.kang@bkl.co.kr

This publication is provided for general informational purposes only, and should not be construed as legal or professional advice on any particular matter, nor create an attorney-client relationship. Before you take any action that may have legal implications, please inquire with your contact at Bae, Kim & Lee LLC, or the authors of this publication.