EU Data Act

As a data processing service provider, Liferay supports the EU Data Act (Regulation 2023/2854/EU), which strengthens the rights of EU customers using cloud-based services and promotes the development of a fair and open cloud-based ecosystem. In line with this, we ensure compliance with the provisions of the Data Act applicable to cloud service providers as follows.

Freedom to Switch Providers (Freedom from Vendor Lock-in)

1. Removing obstacles

The Data Act requires cloud service providers to remove obstacles that hinder switching. At Liferay, we believe that our customers should stay with us because of the quality of our offerings and services, not because of technical limitations.

We provide technical solutions necessary for the proper extraction of data, thereby ensuring that our EU customers can switch service providers at any time without technical obstacles.

Our processes ensure the continuity required during provider migration, helping EU customers migrate their data and applications to a different environment.

We have structured our contractual framework to ensure that our EU customers are afforded the full range of contractual rights required by the Data Act.

2. Who is entitled to switch under the Data Act?

Customers to whom Liferay provides cloud-based services in the European Union.

3. What data can be exported?

Exportable data and digital assets mean customer content, customer application and those elements to which the EU customer has the right of use and which they need in order to be able to use their data effectively in the environment of a new service provider to which they have switched. For clarity, exportable data and digital assets do not include assets or data protected by intellectual property rights, or constituting a trade secret of Liferay or third parties, or data that could compromise the security or integrity of cloud-based services.

4. What does the switching process look like?

For PaaS customers: After opening a support ticket and filling out our switching request form, customers can either download a full backup of their environment through the Liferay Cloud Console or customers can programmatically export and import their exportable data and digital assets using APIs and a batch framework in formats that comply with industry standards.

For SaaS customers: After opening a support ticket and filling out our switching request form customers can either request a full backup copy of their environment data, which Liferay will prepare and deliver or customers can programmatically export and import their exportable data and digital assets using APIs and a batch framework in formats that comply with industry standards.

For Analytics Cloud customers: After opening a support ticket and filling out our switching request form customers can self-serve their data export at any time via the LDP Export API. The following data categories are available for export by active customers via the LDP Export API:

- Event data
- Identity data
- Individual data
- Membership data
- Page data
- Segment data
- Account data

5. Understanding Customer Data and Platform Architecture

Liferay is an open source platform, which means customers have full transparency into how customer data is structured and stored. As outlined in the EU Data Act, Liferay is under no obligation to develop new technologies, rebuild services in a destination provider's environment, or ensure functional equivalence. However, because Liferay is open source, customers already have access to everything they need to understand their data and plan their migration.

Source Code: The full Liferay DXP source code is publicly available at https://github.com/liferay/liferay-portal/tree/master/. Customers can inspect the database schema, data models, service definitions, and internal architecture directly in the codebase. This gives them complete visibility into how their data is structured, how entities relate to each other, and what formats are used internally.

Documentation: Comprehensive product documentation is available at https://learn.liferay.com, covering platform architecture, data management, APIs, configuration, and more. This is customers' primary resource for understanding how to

work with their data, use the available APIs, and plan any data extraction or migration strategy.

Open Interoperability: In accordance with Chapter VIII of the Data Act, Liferay supports interoperability between cloud services. Our platform is built on industry standards that facilitate interoperability, thereby avoiding the lock-in associated with proprietary formats. This commitment to architectural openness guarantees that our customers can effectively manage their digital assets and execute a smooth transition to an alternative environment should their business requirements change. Liferay's REST APIs and Headless framework follow open standards and are fully documented. The API schemas, endpoints, and data formats are available both in the source code and through the platform's built-in API Explorer, allowing customers or their destination provider to understand exactly what data is available and how to retrieve it programmatically.

By combining these resources — the open source code, the public documentation, and the available APIs — customers and their destination providers have all the information necessary to plan and execute a switching process independently.

6. ICT infrastructure and data jurisdiction

In compliance with the EU Data Act, Liferay provides the following information regarding Liferay's cloud-based infrastructure:

Customer Choice of Residency: Each customer has the right to select their preferred data region during the service activation process to ensure alignment with their internal policies. Please note that this choice applies exclusively to the primary hosting infrastructure; the backup storage location is pre-determined and cannot be customized by the customer.

Infrastructure Provider:

- Primary hosting: Google Cloud Platform
- Backup storage: Amazon Web Services

Applicable Jurisdictions: Data processing is primarily subject to the laws of the country where the data center chosen by the customer is located and data is otherwise processed as further outlined at https://www.liferay.com/legal/cloud-services-data, and, where Liferay sells services to its EU based customers, the regulations of the European Union.

Self-Service Monitoring: Customers can independently verify their active primary data center location at any time via the Liferay Cloud Console under the *Settings / Environment* section.

Protection against unlawful international governmental access and transfer of non-personal data

Chapter VII of the Data Act sets forth strict requirements to prevent access to non-personal data requested by non-EU government bodies. Accordingly, Liferay protects the non-personal data stored with us against unlawful access requests from non-EU government agencies through strict technical (encryption, access control) and legal safeguards, in compliance with EU data security requirements.

1. Legal safeguards:

- Liferay evaluates each request individually. We only recognize any decision or judgment issued by an authority in a country outside the European Union that requires Liferay to transfer non-personal data or grant access to such data if it is based on an international agreement in force between the requesting third country and the European Union or between the requesting third country and a Member State, or in the absence of such agreement the request meets the safeguards required by the EU Data Act.
- Liferay challenges the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unenforceable or unlawful, and pursue available possibilities of consultation and appeal.
- If an authority from a third country requests access to your non-personal data, our company is required to notify you. We may only delay this notification in exceptional cases where it would directly jeopardize the success of an ongoing criminal investigation.
- Liferay provides the minimum amount of information permissible when responding to a data request.

2. Technical and organizational safeguards:

- Customer data is primarily stored on Google Cloud Platform, and the data is only accessible for service delivery purposes using strictly secured workstations featuring disk encryption, constant monitoring, and a prohibition on any local or unauthorized device storage.
- System access is secured through centralized identity management and MFA, enforced by strict password policies and restricted firewall rules, while privileged access is limited to select administrators and all activity is continuously tracked via audit logs.

- Customer data is protected through comprehensive isolation: all databases and project environments run on segregated virtual machines and private networks, while production and test systems are logically and physically separated, with a strict prohibition on using production data for development.
- All data, including live systems and backups, is encrypted at rest and only secure network transport protocols are permitted for data transfers.
- Access logs are provided and tamper-protected by Google Cloud Platform, while the Liferay DXP service records the identity, date, and time for every creation or modification of customer data.
- More information on the technical and organizational measures can be found here: https://www.liferay.com/legal/cloud-services-data.

Questions or Concerns?

If you have any further inquiries relating to our Data Act compliance, please address them to legal@liferay.com.