Liferay®

Accelerate Compliance, Protect Your Investments, and Secure Operations with a Liferay Enterprise Subscription

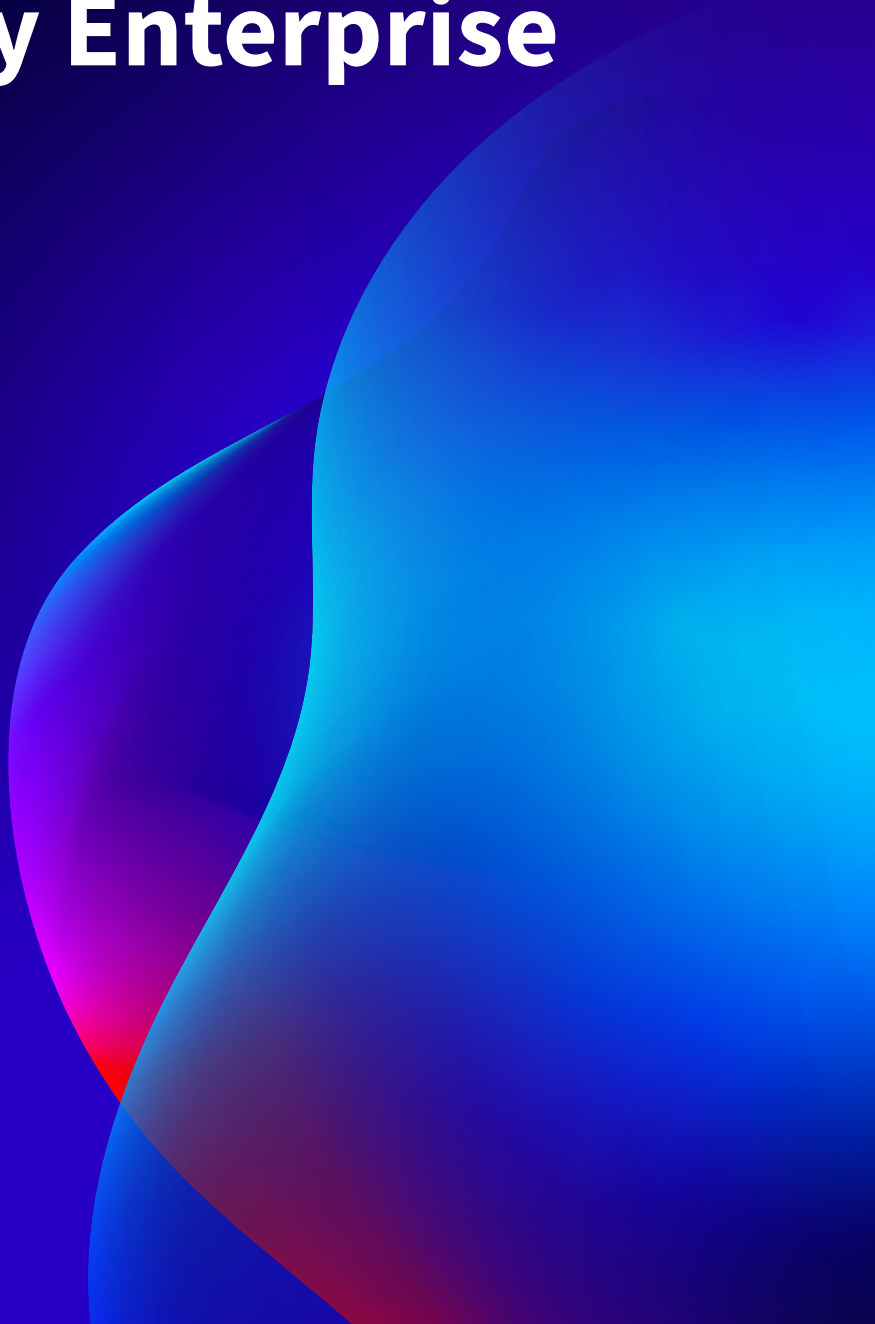

Table of Contents

Achieve Peace of Mind with Liferay 01

How Does a Liferay Enterprise Subscription Accelerate Compliance, Protect your Investments, and Secure Operations? 01

- IP Compliance 02
- Liferay Legal Assurance Program 02
- FOSS Compliance 03
- Dual Licensing Option 05

Security Compliance 05

- Cloud Certifications 05

Data Protection Compliance 06

- General Principles 06
- Specifics for Liferay SaaS and PaaS Deployments 07
- Additional Data Protection Topics 07
- Digital Operations and Resilience 08

Other Compliance Topics 09

Protect Your Investments, Secure Operations, and Lower Total Cost of Ownership 09

Let Liferay Be Your Partner and Catalyst for Innovation 10

Achieve Peace of Mind with Liferay

With the increasing reliance on software and other digital tools comes an increasing need for organizations to ensure that the systems they use adhere to various statutory, regulatory, and industry standards. Effective compliance reduces financial, operational, reputational, and business risks and allows businesses to focus on their operations, rather than worrying about the repercussions of non-compliance.

But compliance can be increasingly difficult to navigate, especially as technologies and regulations continue to evolve in scope and frequency, and nearly impossible to do alone.

Following our mission to make technology useful, our Liferay Subscription Services are designed to provide peace of mind by mitigating non-compliance risks and to allow our customers and partners to reach their full potential by focusing on their business.

We are committed to being more than just a vendor; we aim to be a trusted partner and catalyst for innovation and change for our customers.

How Does a Liferay Enterprise Subscription Accelerate Compliance, Protect your Investments, and Secure Operations?

Open source software is a powerful tool for users aiming for user-driven innovation, tailored use cases, and transparent, secure, and sustainable compliance. However, especially when compared to proprietary tools, open source software presents certain challenges that need to be efficiently managed in order to maximize the many benefits of open source, including lower costs and faster speed to market. That's not even mentioning the increasing regulation and security concerns, escalating the demand for digital governance.

So helping our customers meet their compliance goals, while capitalizing on the benefits of open source software, is therefore an important value proposition of our subscription services. We invest heavily in this area because we believe our team can achieve high compliance standards at scale, and then offer customers these standards as a part of our subscription services. The resulting cost savings on the customer side add to the substantial return that customers see on their investments in Liferay Subscription Services.

This return includes lower total cost of ownership, greater operational security, increased business continuity, higher agility, and faster speed to market compared to unsubscribed users of Liferay.

As a global company serving enterprise customers in the most compliance-driven industries around the world over two decades, we understand that compliance demands will vary based on various factors such as territory, industry, and company size. In addition, each company will have its own compliance focus areas based on its specific risk profile and risk appetite.

Therefore, in this whitepaper, we want to focus on the topics that come up most often for ourselves, our customers, partners, and other users of open source and data processing technology. We'll cover how an enterprise subscription for Liferay DXP will help you meet IP and FOSS compliance, security, data protection, and other data-related compliance and governance topics.

IP Compliance

Open source community development models trade control of the development process for supercharged innovation, better performance, and greater speed to market.

While open source software licenses provide broad freedoms to the users to use, copy, modify, and distribute the software, they also do not include warranties, indemnification, or other remedies in case of a violation of third party IP rights. Each company will approach this lack of control and legal assurances differently depending on the risk profile of the use case, available risk mitigation solutions and the risk appetite. Larger companies may have, for example, open source clearing offices, require license and code scans, and seek assurances from commercial vendors.

Additionally, many companies may require a detailed inventory of all the components, libraries, licenses, and dependencies that are used within software applications. This has become more common in recent years as transparency, security, compliance, and risk management demands in the industry continue to increase. This trend is also underlined by recent regulatory changes, for example, in the USA with **US Presidential EO #14028** and **#14144**, as well as the **Cyber Resilience Act (CRA)** in the EU or SEBI CSRF in India.

A Liferay enterprise subscription is designed to mitigate the risks that come from the lack of control and legal assurances. Through the enterprise subscription, customers are able to satisfy their transparency, security, and regulatory compliance demands through our Liferay Legal Assurance Program, FOSS compliance, and dual licensing options.

Liferay Legal Assurance Program

Our Legal Assurance Program is not merely a statement of our commitment to foster trust and protect our subscription customers and partners, but a contractually binding safeguard. Liferay's Legal Assurance Program mitigates the lack of single vendor development control and legal assurances in two key ways.

First, in case of a third-party infringement claim, Liferay defends its customer against the claim similar to what you see from traditional proprietary software vendors. Secondly, and more importantly, the program also focuses on business continuity as Liferay commits to respond to claims, by either acquiring the necessary IP rights, or by modifying or replacing the affected code with non-infringing code. This program is not a separate add-on, but already included as an integral part of a Liferay Enterprise Subscription.

Compared to similarly situated commercial open source vendors, Liferay's Legal Assurance Program covers a broader range of intellectual property claims, including copyrights, trademarks, and patents. Moreover, the Legal Assurance Program is not geographically limited but applies globally.

FOSS Compliance

Free and Open Source Software (FOSS) compliance requires users of FOSS to observe all the copyright notices and satisfy all the license obligations for the FOSS they use in commercial products.

Compliance with these FOSS obligations and the increased transparency, security, compliance, and risk management demands in software development and supply chain management, including those resulting from new regulation as mentioned above, require users to produce a detailed software inventory list in the form of a Software Bill of Materials (SBOMs). Producing these SBOMs requires scanning tools or services, knowledge and diligent review, and human resources.

As a part of Liferay's Enterprise Subscription, subscribers get access to software bills of materials (SBOMs) of everything that goes into a Liferay DXP package, in both SPDX (ISO/IEC 5692) and CycloneDX (ECMA 424) formats using state-of-the-art end-to-end pipeline of the software composition analysis (SCA) tool, ScanCode.io.

This helps our customers mitigate the costs required to scan and review source code. Based on our customers' experience, this is hundreds of thousands of dollars and hundreds of man-hours per year.

Liferay applies the following standards and industry best practices in our FOSS and general IPR compliance:

SPDX (ISO/IEC 5692) – Software Package Data Exchange is an open standard capable of representing systems with software components in SBOMs (Software Bill of Materials) and other AI, data and security references supporting a range of risk management use cases. To our Liferay DXP customers, we offer SBOMs in SPDX 2.3 JSON format, which they can self-serve directly from Liferay's Customer Portal.

OpenChain (ISO/IEC 5230) is an international standard for open source license compliance programs, which certifies that Liferay has appropriate policies, processes and people in place to assure open source license compliance. Liferay has been conformant since 2019, being an early adopter even before OpenChain became an ISO standard.

REUSE.software are community/ industry best practices (based on SPDX) on how to equip one's own source code with copyright and license information that is both human- and machine-readable. By adopting this specification in our internal licensing policies, Liferay enables everyone relying on its source code to have a clear and concise picture of which files they may use in what way.

ScanCode.io is a highly regarded SCA (Software Composition Analysis) tool and license scanner. We use it to automatically scan every Liferay DXP package by comparing the binary build with the source code of DXP and its whole dependency tree, before we release it to our customers. The results of a (successful) scan end up in an SBOM in both SPDX and CycloneDX format, that we offer to our Liferay DXP customers and partners through Liferay's Customer Portal.

CycloneDX (ECMA 424) is another international standard SBOM format. To our Liferay DXP customers, we offer SBOMs in CycloneDX 1.6 (JSON) format, which they can self-serve directly from Liferay's Customer Portal.

Liferay doesn't just follow these industry best practices, but is also involved in shaping them. For example, SPDX, OpenChain, and REUSE.software include contributions from our legal team. Liferay also sponsored the development of the advanced **"map-deploy-to-develop" pipeline**, which we use to analyze what exactly goes into our packages. This enables us to provide customers, partners, and members of the open-source community with comprehensive and precise SBOMs.

Dual Licensing Option

Customers have the option to use Liferay DXP under either a Liferay commercial license (DXP EULA) or a LGPL-2.1-or-later license.

This does not affect the fact that the license is provided without a license fee and on perpetual terms. So only additional subscription benefits will stop at the end of a subscription term, not the actual license.

The dual licensing option may be helpful for customers and partners who want to minimize the compliance overhead associated with using open source licensed software. It is also useful for customers who are concerned about compatibility with other code, if they feel the open source license might not be suitable for a specific project or their go-to-market strategy.

Even customers who have established their own open source licensing policies and OSPOs (Open Source Programme Offices) of their own, can accelerate procurement, negotiation, and compliance communication considerably under this licensing option.

Security Compliance

Liferay has made security a priority for both our software platform and company operations so that you can build your business operations upon a platform you can trust.

Security compliance refers to a set of practices and measures taken to ensure the confidentiality, integrity and availability (CIA) of systems and information belonging to Liferay or entrusted to Liferay by its customers. At Liferay, we approach security through our certified Information Security Management System (ISMS).

Cloud Certifications

Running compliant operations in the cloud means adhering to a set of regulations and standards established by governing bodies, industry groups, or internal policies aimed to safeguard sensitive data, ensure data privacy, and maintain the integrity of cloud services.

For Liferay products that include cloud-based services, Liferay maintains third-party certifications including:

- **ISO/IEC 27001, 27017, 27018:** These certificates tackle information security from different angles, and work together to create a robust security system.
- **CSA Star Level 1 & 2:** This certification program was created by the Cloud Security Alliance (CSA) to help organizations assess and improve their cloud security posture. Level 1 is Self-Assessment, and Level 2 is Third-Party Audit.
- **SOC 2 (Service Organization Controls):** A widely used standard for assessing the security posture of a service organization.

- **HIPAA (Health Insurance Portability and Accountability Act):** Protects the privacy of individually identifiable health information (PII) in the healthcare industry.
- **Esquema Nacional de Seguridad (ENS):** Ensures the security of digital services and data for public administrations and private sector entities working with them in Spain.

Data Protection Compliance

General Principles

Data protection compliance focuses on securing personal data and preventing any use of that data in a way that could harm individuals. Liferay acknowledges the complexity of data protection compliance. That's why we not only maintain organizational adherence to data protection laws but also embed features and functionality that give users options and controls over protecting data within our products. Our products are designed to support our customers' efforts to achieve compliance against common data protection standards within their own operations.

When handling personal data as part of our cloud-based offerings, Liferay pledges to process such data in line with key data protection frameworks, a commitment enshrined in our agreements.

- **Strong Security Measures:** Liferay is committed to adopting and maintaining robust Technical and Organizational Measures to ensure the security of personal data.
- **Purpose-Driven Data Processing:** Liferay processes personal data solely and strictly as instructed by our customers.
- **Vetted Sub-Processors:** Our agreements only allow us to engage sub-processors who are subject to equivalent standards of data protection guaranteeing, where applicable, the relevant data transfer mechanisms. Liferay only engages sub-processes after extensive due diligence review.
- **Export & Deletion of Personal Data:** Liferay facilitates the exportation or deletion of personal data at the end of a subscription term and aids customers in responding to data subject requests.
- **Audit Collaboration:** Liferay pledges cooperation with our customers during audits to verify compliant data processing practices.
- **Breach Communication:** In the event of a data breach, Liferay ensures timely and comprehensive communication with affected customers, minimizing potential impacts.

Liferay's commitments, outlined in our agreements, reflect our proactive stance on data protection and our dedication to supporting our customers' data protection compliance efforts.

Specifics for Liferay SaaS and PaaS Deployments

Our enterprise subscription allows you to choose to deploy Liferay DXP any way you need: on-premise or self-hosted cloud models, or in Liferay Cloud Infrastructure. Our cloud-based subscription options, Liferay PaaS and Liferay SaaS, are backed by Google Cloud™, meaning data security, such as encryption at rest, is handled by a reliable vendor with world-class and secure technology. Our partnership with Google also allows us to provide additional security features to filter web traffic and secure your solutions from cyberattacks, such as DDoS protection, a CDN, load balancing, and a WAF.

Applications running on Google Cloud Platform (GCP) can achieve data sovereignty compliance through a combination of GCP's and Liferay features, including:

- **Data Residency:** This is a core aspect. GCP allows you to choose the geographic region where your Liferay data (user data, portal content, etc.) is stored. This ensures your data stays within the boundaries you define and complies with local regulations.
- **Google Cloud Sovereign Cloud:** For the most stringent requirements, Google provides a Google Cloud Sovereign Cloud option with local delivery partners to increase trust and transparency through local partners managing the sovereign cloud infrastructure.
- **Regional Controls:** Even within GCP's global infrastructure, you can implement security controls for specific folders within a region. This can be helpful if your data needs to comply with regional regulations within a broader geographic area
- **Data Encryption:** Utilize encryption options to encrypt your data at rest and in transit to protect the data from third parties.
- **Liferay User Access Controls:** Leverage Liferay Cloud Infrastructure console's built-in user access controls to restrict access to data based on the principle of least privilege. This ensures only authorized users can access specific data within your Liferay portal.

With Liferay SaaS, general security tasks can be further offloaded to the Liferay team to handle, including performance monitoring, backups, platform upgrades, and disaster recovery. These tasks can also be offloaded to the Liferay team for Liferay PaaS customers with the **Premium Security add-on subscription**.

Additional Data Protection Topics

Though no software product can offer a checklist of features to make your company completely compliant with the data protection laws, Liferay DXP provides tools to greatly accelerate a company's journey towards compliance. With out-of-the-box features such as data export, data erasure, and user permissions combined with Liferay DXP's flexible architecture, businesses can adapt the platform to the evolving needs of their data protection strategy.

For example, Liferay's User Associated Data (UAD) framework helps your organization meet two of the General Data Protection Regulation's (GDPR) most technically challenging requirements:

- **The right to data portability.** Users have the right to receive their personal data in a machine-readable format.
- **The right to be forgotten.** Organizations can remove the ability (even for administrators) to glean information that could lead to knowing the identity of the user whose personal data was erased or anonymized. This mainly consists of deleting the identity information from the system and erasing or anonymizing content the user has interacted with, so it cannot be tracked to a real person.

Additionally, you can ensure GDPR compliance for your cookies by selecting Explicit Cookie Consent Mode within Liferay DXP's configuration interface. You can also customize the text that will appear to display your company's cookie and privacy policies.

For a more detailed dive into how Liferay enables compliance with the requirements under GDPR, specifically, read more **here**.

Digital Operations and Resilience

We strongly believe that leveraging the commercial support of a trusted vendor for open source software deployments can be a valuable strategy to meet compliance requirements under application law or regulation, like the EU Digital Operational Resilience Act (DORA).

Liferay's subscription services can help you meet your digital operations and resilience requirements in several aspects, including:

- **Risk mitigation and resilience:** Support for Liferay's commercial offering includes defined Service Level Agreements (SLAs), which is crucial to meet incident reporting and recovery requirements.
- **Vulnerability management including continuous monitoring requirements:** Liferay provides proactive and continuous third party software, including open source software, tracking guidance on patching and vulnerability awareness.
- **Third-party risk management:** Liferay places security at the heart of our operations so you can get the assurances you need that your supply chain meets the same resilience standards as you are.
- **Expertise and auditability:** With our team's expertise and documented compliance, we can help you showcasing a structured approach to managing open-source software within the ICT ecosystem.

Other Compliance Topics

As noted in the beginning of this document, compliance demands will vary based on various factors and we have only focused on topics that we see as most relevant for our customers. If you are looking for additional information regarding Liferay's compliance efforts and ethical standards you will find additional information regarding many topics such as our Code of Conduct and Ethics Anti-Corruption Policies or ESG Governance at our **Trust Center**.

Protect Your Investments, Secure Operations, and Lower Total Cost of Ownership

The base subscription cost or initial investment of a technology is not the only cost that has to be considered when evaluating a solution. You also need to take into account the resources and responsibilities of managing, supporting, and evolving that technology, including meeting legal, industry requirements, and customer expectations.

The compliance benefits that come with an enterprise subscription, as outlined in this whitepaper, will help reduce your total cost of ownership and protect your investments and operations.

The price for FOSS compliance — which may include subscribing to scanning tools, using scanning services to pay for legal review, maintaining updated and compliant SBOMs, or making code available for download — may be far greater than the cost of a subscription when taking into account these tools, the underlying infrastructure, and human expertise needed.

On top of these expenditures, you need to factor in the potential costs of regulatory fines, defending third-party infringement claims, risk of damages, loss of reputation, or interruption of operations. In comparison, the cost of a subscription becomes an investment that can provide excellent ROI, risk mitigation, and ultimately peace of mind.

On the security and data protection side, subscription-exclusive security features and certified standards present additional risk mitigation. And, instead of needing to handle security tasks on your own or stay on top of new vulnerabilities, you can rely on Liferay to protect the platform by monitoring for security vulnerabilities and implementing fixes for the software.

Customers leveraging our SaaS subscription option will get these security patches and fixes applied for their instance by the Liferay team. All of this saves you costs for human and technical resources and allows your organization to focus on supporting your business. Additionally with our quarterly release cycle, you'll be able to take advantage of new features and updates regularly avoiding potentially costly extended time periods with security vulnerabilities.

Let Liferay Be Your Partner and Catalyst for Innovation

Compliance doesn't need to be a challenge you navigate on your own. With a Liferay Enterprise Subscription, you gain access to the support and experts you need to accelerate the compliance of and protect the investments in your products and digital solutions. Offload some of the burden and let Liferay be a trusted partner in your digital compliance efforts and a catalyst for innovation.

To learn more about our compliance and security programs, visit our **Trust Center**.

To learn about other subscription benefits, see our Benefits of an Enterprise Subscription whitepaper **here**.

Liferay helps organizations build for the future by enabling them to create, manage, and scale powerful solutions on the world's most flexible Digital Experience Platform (DXP). Trusted globally by over a thousand companies spanning multiple industries, Liferay's open-source DXP facilitates the development of marketing and commerce websites, customer portals, intranets, and more. Learn how we can use technology to change the world together at liferay.com.