GDPR Compliance

Addressing the unique challenges of software product companies operating with global teams

Compliance

99x.io

As a C-Level executive, any lapse in data privacy or information security can jeopardize not only your product but also your career. Achieving GDPR compliance poses significant challenges for software product companies. As product companies handle vast amounts of personal data, they must navigate a complex regulatory landscape to ensure they meet GDPR requirements. From managing data subject rights to maintaining robust data protection practices, the path to compliance requires careful planning, ongoing monitoring, and continuous adaptation. This paper discusses unique challenges that software product companies face in their quest to comply with GDPR.

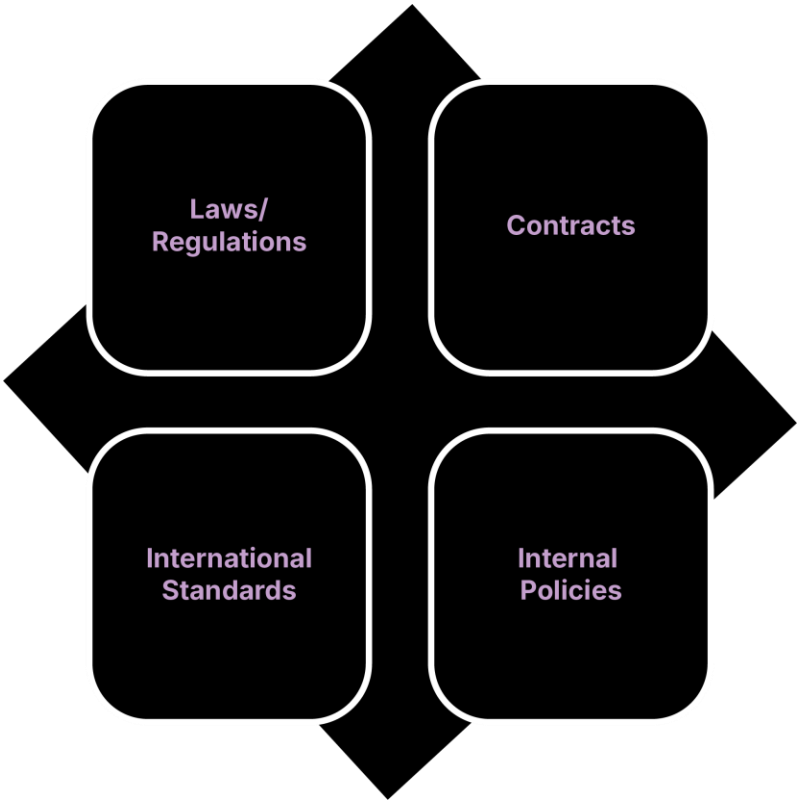
An overview of GDPR requirements

The General Data Protection Regulation (GDPR) is a comprehensive data protection law enacted by the European Union (EU) to enhance individuals' control over their personal data and unify data protection regulations across EU member states. Seven key principles of GDPR are:

- **Lawfulness, Fairness, and Transparency:** Data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization:** Data collected should be adequate, relevant, and limited to what is necessary for the intended purposes.
- **Accuracy:** Data must be accurate and kept up to date, with every reasonable step taken to ensure inaccurate data is erased or rectified.
- **Storage Limitation:** Data should be kept in a form that permits identification of individuals for no longer than necessary.
- **Integrity and Confidentiality:** Data must be processed securely to protect against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability:** Organizations are responsible for complying with these principles and must be able to demonstrate their compliance.

Data Privacy and Security Compliance at 99x

99x's compliance program, based on ISO integrated management system, primarily aims to prevent and detect violations of laws, regulations, and internal policies that could cause legal or reputational damage to the organization. It also fosters a culture of ethical behavior and responsible decision-making. Our compliance program covers the following four focus areas:



Legal and regulatory compliance:

To ensure adherence to all applicable laws and regulations such as EU GDPR to avoid legal penalties and maintain the organization's integrity.

International standards compliance:

To align the organization’s practices with recognized international standards such as ISO to enhance credibility and competitiveness in the global market.

Contractual compliance:

To monitor and manage the organization's obligations under various contracts to avoid breaches and maintain good relationships with various stakeholders including partners, customers, employees, and suppliers.

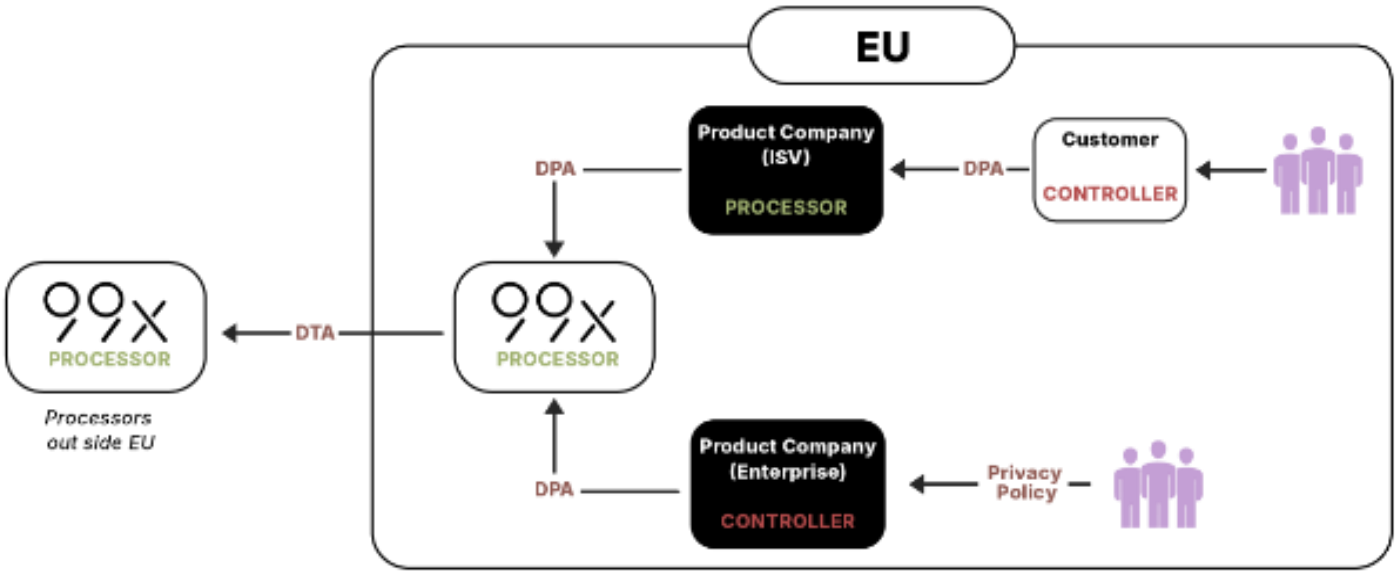
Policy compliance:

To enforce internal policies to ensure consistent and ethical behavior throughout the organization.

In the successful implementation of a Privacy Management Framework, the role of the Data Protection Officer (DPO) at 99x is crucial. The DPO ensures that the organization remains vigilant in meeting GDPR requirements, advising on privacy matters, monitoring compliance, and serving as a point of contact for regulatory authorities. A robust, organization-wide Data Protection Policy provides the foundation for privacy compliance. It sets clear directives for how personal data is handled, guiding employees at every level to ensure a unified approach to data protection.

GDPR roles and obligations as a product company

Product companies, whether they are independent software vendors (ISVs) or enterprises subject to GDPR, will play one of two roles: **data processor** or **data controller**, depending on their proximity to the data subjects in the personal data flow. The figure below illustrates the roles of a product company when 99x is engaged as the outsourcing partner, along with the personal data flow and the necessary legal controls that must be in place.



Data controllers are generally tasked with deciding the purposes and methods of processing personal data, whereas data processors are responsible for executing the processing activities on behalf of the data controller.

Six GDPR activities product companies must address

Given below are the key unique challenges that software product companies might face in their quest to comply with GDPR.

1. Identifying features that are subjected to GDPR compliance:

Product companies face the challenge of designing and developing features that not only meet user needs but also comply with GDPR requirements. This involves identifying which aspects of the product will interact with personal data and ensuring those features include mechanisms for lawful data processing, such as consent management, data access controls, and data minimization techniques. Companies must also consider how features like data deletion, data portability, and user profiling are implemented to align with GDPR principles.

2. Implement Privacy by Design and Privacy by Default principles:

Adhering to the GDPR principles of Privacy by Design and Privacy by Default requires product companies to embed privacy considerations into the very fabric of their software development processes. Privacy by Design means considering privacy from the earliest stages of product development and making it an integral part of the overall design. Privacy by Default requires that the default settings of any product or service ensure that no more data than necessary is processed.

3. Engineering personal data security:

Ensuring the security of personal data is a fundamental requirement under GDPR, and for product companies, this means engineering robust security mechanisms within their products. This includes implementing encryption, access controls, and secure data storage methods to protect against unauthorized access, data breaches, and other security threats.

4. Implementing relevant data processing agreements:

Product companies must navigate the complexities of data processing agreements (DPAs) when collaborating with third-party processors. These agreements outline the responsibilities and obligations of both parties concerning the handling of personal data. Companies need to ensure that DPAs are in place with all third parties involved in data processing activities, clearly defining how personal data will be processed, secured, and accessed.

5. Implementing relevant data transfer agreements:

When transferring personal data outside the European Economic Area (EEA), product companies must ensure that adequate safeguards are in place to protect that data. This involves implementing data transfer agreements, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), to ensure that data transfers comply with GDPR requirements. Product companies must be vigilant in assessing the legal landscape of data transfers, especially in light of evolving regulations and court rulings.

6. GDPR Compliance status of the outsourced service providers (such as 99x):

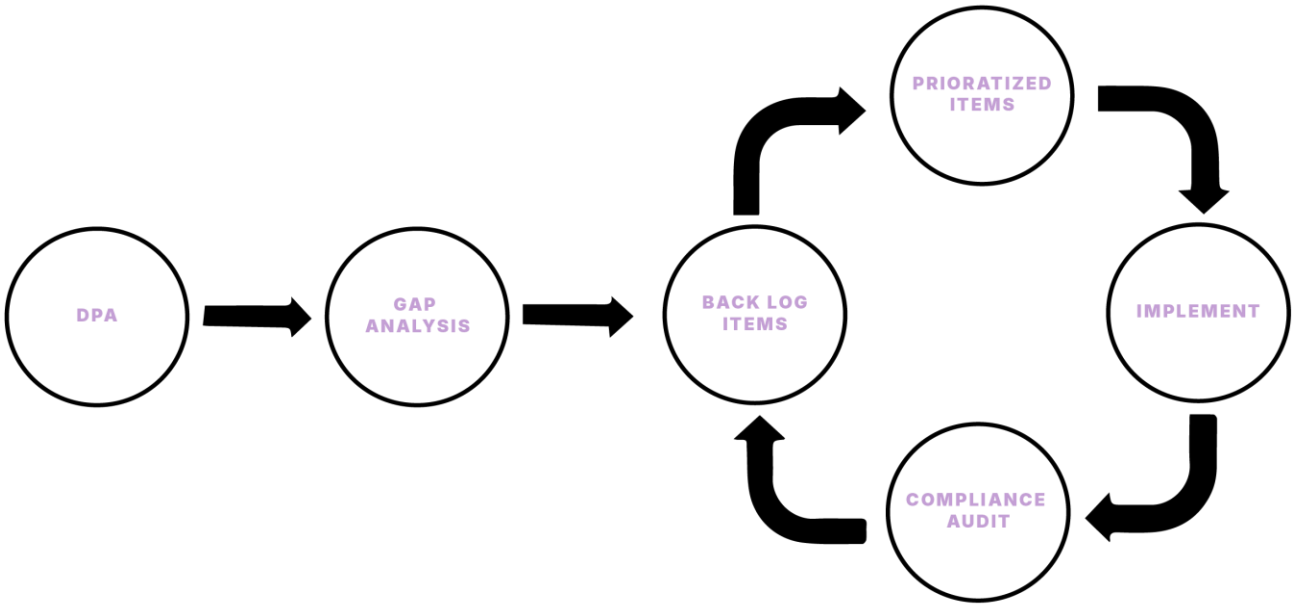
Product companies often rely on outsourced service providers to handle various aspects of their operations, including software engineering, testing, and maintenance. Ensuring that these service providers comply with GDPR is a critical challenge, as any non-compliance by a third party can lead to significant legal and financial repercussions for the product company.

Enabling GDPR Compliance through ISO 27701

Navigating the requirements of GDPR compliance presents a considerable challenge for businesses. However, adopting international standards such as ISO 27701 can serve as a powerful strategy to address this issue. ISO 27701 provides a framework for privacy management, helping businesses systematically protect personal data and ensure regulatory compliance. By integrating this standard, organizations can streamline their compliance efforts, reduce risks, and build a robust data protection infrastructure. ISO 27701 extends ISO 27001 and ISO 27002 by adding requirements and guidance specific to privacy and the management of personal data. It specifies requirements for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

Customer Engagement Process

At 99x, we prioritize a seamless and transparent approach when it comes to engaging with our customers. Our commitment to GDPR compliance and data protection is reflected in each phase of our interaction. Here's how we guide our clients through this journey of GDPR compliance:



DPA - Data Processing Agreement

Our Business Development representative presents the Data Processing Agreement (DPA) alongside the business contract to ensure early alignment on data protection protocols. Carefully crafted in consultation with leading Norwegian legal experts, 99x offers a comprehensive DPA template designed to meet legal and operational standards. We understand that the flexibility is key—our customers are free to use this template or opt for their legal counsel's recommendations, fostering an adaptable partnership grounded in mutual trust.

Gap Analysis

Achieving compliance with GDPR is integral to every project. Together with the customer's designated representative, our 99x Delivery Manager leads a collaborative GDPR gap analysis exercise. Leveraging the ISO 27701 privacy control framework and the expertise of the 99x compliance team, this analysis identifies any discrepancies in the current practices, ensuring that our approach is both proactive and aligned with the latest regulations.

Backlog of Tasks

Based on the outcomes of the gap analysis, our Team Lead identifies critical tasks that need to be addressed, ensuring every compliance challenge is documented and tracked. This backlog serves as a blueprint for delivering on privacy and data protection goals, clearly laying out the next steps.

Prioritizing Tasks

The Product Owner works closely with stakeholders to prioritize the backlog items, ensuring that resources are efficiently allocated and key compliance tasks are addressed promptly. This structured approach ensures that compliance initiatives align seamlessly with business goals.

Periodic Audits

At 99x, we believe in continuous improvement. Our Compliance Team conducts internal privacy audits every six months to evaluate ongoing compliance with privacy regulations. Any gaps identified are promptly escalated to relevant stakeholders, guaranteeing that corrective measures are taken without delay, reinforcing our commitment to maintaining a high standard of privacy and data protection.

Enabling GDPR Compliance with ISO 27701

Navigating the requirements of GDPR compliance presents a considerable challenge for businesses. However, adopting international standards such as ISO 27701 can serve as a powerful strategy to address this issue. ISO 27701 provides a framework for privacy management, helping businesses systematically protect personal data and ensure regulatory compliance. By integrating this standard, organizations can streamline their compliance efforts, reduce risks, and build a robust data protection infrastructure. ISO 27701 extends ISO 27001 and ISO 27002 by adding requirements and guidance specific to privacy and the management of personal data. It specifies requirements for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

Privacy requirements are not an optional extra!

As a Product Manager, CEO or CTO, this is not an area that you can take lightly. The cost of a privacy breach is huge - enough to cripple your company and your career. Does your tech partner provide you the peace of mind regarding your data privacy considerations? Are the necessary safeguards in place? At 99x, our privacy by design and internal compliance processes ensure your data privacy related challenges are addressed.

99x : Co-creating Winning Product Experiences

We empower Digital Product Vendors to create Winning Product Experiences through our Facilitated Teams. By combining our expertise in **product engineering** and **product design**, we co-create products that achieve **market-fit** and **drive adoption**. Our Facilitated Teams provide clients with the capacity, competence, convenience, compliance, and cost-effectiveness needed for long-term success as their trusted partner. To learn more, download our Winning Product e-book here.

Disclaimer - This white paper is provided for informational purposes only and does not constitute legal advice. While every effort has been made to ensure the accuracy and completeness of the information contained herein, the authors and publishers make no warranties or representations regarding the content's correctness, reliability, or suitability for any particular purpose. Readers are encouraged to seek professional legal counsel to address specific compliance issues and concerns related to the General Data Protection Regulation (GDPR). The authors and publishers disclaim any liability for any direct, indirect, incidental, or consequential damages arising out of or in connection with the use of this white paper. Furthermore, this white paper is not intended to serve as a comprehensive guide to GDPR compliance. Organizations should perform their own due diligence and consult with qualified professionals to develop and implement a compliance strategy tailored to their specific needs and circumstances.