SYNOPSYS®

General Data Protection Regulation (GDPR) Readiness

Avoid GDPR compliance risk by improving the security of the software you use to process data

We provide you tools, insight, and guidance to address these key GDPR requirements:

Article 25: Data protection by design and by default

Article 32: Security of processing

Article 35: Data protection impact assessment

Overview

The European Union (EU) General Data Protection Regulation (GDPR) comprises a set of articles that requires organizations to strengthen their data protection and security measures. All organizations that store, process, or transmit personal data of EU residents must demonstrate compliance with this regulation at all times. Synopsys helps organizations eliminate attack vectors to stop hackers from exploiting weaknesses in application security practices and gaining access to personal data.

If you want to mitigate your risk of GDPR noncompliance due to data breaches, we can help you with any of these activities:

- Establishing or maturing your software security initiative (SSI)
- Augmenting the security posture of the software you use to process EU resident data
- Tracking and managing vulnerabilities in the open source components in your applications
- Evaluating the risks posed by third-party APIs involved in processing personal data
- Starting an application/product security program or focusing on a specific area, such as vendor management, defect management, security tools, or training

GDPR standards are driving a fundamental shift in the risk management of applications, systems, and processes involved in processing personal data. For example, what was once considered a medium- or low-severity vulnerability might now be considered high severity because of the added impact of GDPR noncompliance. Synopsys application security testing tools and services can help you establish reliable measures of risk for your systems and applications and prioritize remediation efforts to ensure consistent protection of personal data.

4 keys to avoiding noncompliance

1. Audit your applications for security issues that could result in a data breach.
2. Track and manage vulnerabilities throughout the software development life cycle (SDLC).
3. Monitor for new vulnerabilities affecting applications, including internal and open source code.
4. Evaluate the security risk in the third-party APIs your applications interoperate with.

No one else offers a more comprehensive portfolio of products, services, and training to support application security compliance.

Product or service	How you can move toward GDPR compliance
Building Security In Maturity Model (BSIMM)	Measure and evaluate a software security initiative (SSI) with a focus on compliance.
Maturity Action Plan (MAP)	Build a detailed plan and roadmap with a prioritized list of recommendations to enhance your software security program.
Policies and Standards Development	Define rules of governance and compliance so you can • Measure the effectiveness of your security program. • Ensure consistent development and application testing. • Establish acceptable security minimums for building and deploying applications.
Threat Modeling and Architecture Risk Analysis	Evaluate applications and systems through the lens of relevant GDPR articles. With a design review focused on safeguarding personal data, you can • Understand the assets in your systems and how well they are protected. • Ensure that even perfectly secure and compliant applications are not doing things with data that don't show up in a pen test.
Security Control Design Analysis	Perform a privacy impact analysis, and build a data inventory.
SAST, DAST, IAST, Fuzz Testing	Evaluate data-processing systems, applications, and services by testing, assessing vulnerabilities, and remediating them to ensure the ongoing confidentiality, integrity, availability, and resilience of data.
Software Composition Analysis (SCA—Black Duck and Protecode SC)	Get open source vulnerability management and on-demand security audits to manage your overall application security risk.
Vendor Building Security In Maturity Model (vBSIMM)	Ensure third-party software meets compliance requirements and protects personal data.
Training	Educate your teams on how to reassess the processes and systems that store, transfer, and process your data.

What you can do with Synopsys as your partner

- Establish or mature your SSI to avoid violating specific GDPR articles that require mechanisms for safeguarding personal data.
- Create well-documented application security processes and procedures to move toward GDPR compliance.
- Gain risk visibility across systems, applications, and APIs.
- Evaluate existing security vulnerabilities, policies, system configuration settings, and privileged access rights.
- Simplify GDPR compliance reporting.
- Minimize the risk of personal data breaches.
- Strengthen application security internal policies and governance.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com