SYNOPSYS®

The 7 elements of GDPR software security compliance

Adam Brown

By now, you're probably aware that the General Data Protection Regulation (GDPR) is coming. Taking effect on May 25, 2018, GDPR aims to unify the European Union (EU) on common data protection practices. Bringing more control and higher standards, this regulation will affect how firms gather, store, and use data pertaining to EU residents.

Let's examine seven steps your firm can take to continuously improve its software security initiative, thus illustrating GDPR software security compliance.

1. Understand how GDPR affects your organization

Regardless of your organization's location, whether it operates primarily inside or outside the EU, if it uses data relating to EU residents, then GDPR applies to you. Transactions can include any operations carried out with employees, other organizations, and customers—even those receiving a free service.

Article 35, "Data protection impact assessment," stipulates that prior to data processing, an assessment of the measures envisaged to address the risks, including security measures and mechanisms, must be performed.

To comply with Article 35, organizations processing personal EU data should do the following:

- **Mitigate risk appropriately.** One way to get started is by carrying out a Building Security In Maturity Model (BSIMM) assessment. The BSIMM is a benchmarking activity that provides an objective, data-driven perspective of your firm's current software security and compliance operations—thus providing measurable visibility into areas that could benefit from improvement.
- **Enact a defense strategy in the event of a breach.** Address your unique security and quality needs so that you can resolve vulnerabilities and prevent issues before they occur. It's also highly beneficial to build a defense strategy with experts so that your firm can be prepared in case a breach does transpire.

2. Know your organization's obligations under GDPR

Organizations are obligated to demonstrate GDPR compliance. But how? That's the question firms are asking.

Some key obligations

- Keep records of all data processing activities and the reasons behind them
- Conduct an impact assessment to measure the risk to data privacy and evaluate the measures and mechanisms in place to secure it before any data is processed (Article 35)
- Review this assessment carefully to determine whether its processing security standards can evolve as the risk landscape changes (Article 35)
- Implement measures for privacy by design (depending on the sensitivity of the data)
- Comply with new requirements around transparency, fair processing, and notifying individuals of their rights
- Appoint a data protection officer (DPO) where appropriate (Article 37)

3. Determine whether you're a data controller or processor

As with previous data laws, GDPR makes clear distinctions between data controllers (i.e., data owners) and data processors. Each holds a different role. Before creating an action plan to propose to senior leadership, you'll need to figure out whether your organization is a data controller, a data processor, or both.

Is my organization a data controller?

Controllers are responsible for, and must comply with, these principles regarding personal data:

- **Lawfulness.** This is covered largely in Article 6. In summary, data processing must be necessary, and the subject must have given consent.
- **Fairness.** This is a safeguard that changes over time. It requires controllers to take account of the interests and reasonable expectations of data subjects.
- **Transparency.** Organizations must have easily accessible and understandable policies on what processing is done.
- **Storage limitations.** Data can't be stored after it's not needed for the purpose it was originally obtained for.
- **Integrity and confidentiality.** These cover security controls we're already familiar with.

For control issues—that is, what is done with the data (e.g., where it is sent, what kind of processing is done on it)—the buck stops with the controller. Controllers must also be sure data is processed with the correct security controls, whether by their own organizations or by a third-party data processor.

Is my organization a data processor?

Processors must have appropriate technical security measures in place. For example, an ISO 27001 implementation would be a good start. Additionally, as we know, secure software, networks, and environments are essential. The best way to create a culture of software security in an organization is to implement a software security initiative.

4. Obtain buy-in from senior management

Sponsorship and support from your organization's top decision-makers influence real change. Since GDPR will be enforced globally and is accompanied by sizeable monetary penalties for noncompliance, getting buy-in from senior management is critical. Outlining the potential penalty fines, in addition to proposing an actionable strategy to meet the obligations facing your firm, will aid you in obtaining trust and commitment to a program.

5. Carry out data protection impact assessments

Data protection impact assessments (DPIAs) can be an integral part of carrying out privacy by design. However, in some cases, GDPR mandates that a DPIA be carried out, depending on the sensitivity of your data. You may be thinking, "What is this DPIA you speak of?" Fret not. A DPIA is also known as a privacy impact assessment (PIA). In other words, it's something that organizations have been using for years as an effective way to comply with other data regulations.

6. Establish a data protection officer

If your firm is a public authority performing large-scale systematic monitoring of individuals (e.g., online behavior tracking) or running large-scale processing of special categories of data, then you need a data protection officer (DPO). The DPO's role is to inform and advise, monitor compliance, manage internal data protection activities, and be the first point of contact in a breach.

The DPO reports to the board, cannot be penalized for performing their duties, and must have adequate resources for their role. They do not have to be an employee and can be external; in fact, DPO-as-a-service is now a thing.

One focus of the DPO involves securing any piece of software that plays a role in processing personal data. They must also ensure that the organization continuously monitors for new vulnerabilities affecting production applications, per Article 32.

7. Build security and privacy in

Security must be built into the software and systems that personal data passes through, from the start, with documented standards and practices to minimize the attack surface. Article 25 specifically calls for measures to ensure that personal data is not made accessible without the individual's consent (including during a breach).

Ultimately, architectural flaws are by their very nature the most impactful security and privacy challenges that can be discovered. Thankfully, finding them before a system is implemented prevents costly rework.

Still, there are limits to finding design flaws before they've affected implementation. This can happen only during greenfield development (starting from absolute scratch with all-new code) and during the development of new functionality in an existing system.

The more common scenario is that a flaw is discovered in an existing (implemented and fielded) system component owing to ongoing architecture risk analysis (ARA). In these cases, it's doubly important to consider your options for flaw mitigation. Often a stop-gap solution can be placed in a deployed system, while architects work to establish more permanent shifts in design to alleviate the risk more fully.

Summing it up

Keep in mind that GDPR isn't optional. The penalties can potentially devastate an organization. Article 83 sets out a tiered approach to penalties, with a maximum fine for violating GDPR of up to 4% of annual global turnover or €20 million (approximately $24 million), whichever is greater. It's also important to note that GDPR guidelines and penalties apply to any member of the supply chain that processes an EU resident's data.

Turn GDPR risk into a competitive advantage.

Get started

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to 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

SYNOPSYS®
Silicon to Software™

03/28/18.FAQ_7GDPR_032818.