SYNOPSYS®

Silicon to Software™

Data Privacy and Protection Statement

Table of Contents

SYNOPSYS®

SYNOPSYS®

SECTION 1 – INTRODUCTION

1.1 Protecting data is at the core of what we do

Synopsys is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. Not only do we have a long history of being a global leader in electronic design automation (EDA) and semiconductor IP, we are also a leader in helping businesses design secure systems and build security into their software development life cycle.

We take just as seriously our duty to maintain the security and privacy of the personal data of our customers, employees, and vendors to which we have access, and our legal obligations under the data privacy laws of the different countries where we do business. Security and data protection are woven into our organization.

1.2 Everyone is responsible for data privacy and protection

Everyone working on behalf of Synopsys, Inc. and its subsidiary companies (referred to collectively in this Statement as "Synopsys"), including our employees, contractors, and vendors, is expected to apply our principles of data privacy and protection to all of their activities and to comply with our privacy policies. Our privacy principles are presented in Section 2, but in general these principles and policies ensure that we only request personal data for which there is a justifiable business need, take steps to properly secure it, allow access or use only when authorized for legitimate business needs, do not retain it past the point when the legitimate business need has ended, and use a secure method to dispose of it.

1.3 Rights and inquiries

Synopsys employees and others who have questions or concerns about particular practices and compliance with data privacy laws may contact any of the following: the Synopsys Data Privacy Officer, if one has been designated in the country where they reside, the Company's Chief Privacy Officer at privacy@synopsys.com, the Chief Ethics and Compliance Officer at ethics.officer@synopsys.com, or the Synopsys Legal Department.

Integrity is one of Synopsys' core values.
A strong commitment to data privacy and protection is one of the ways we uphold our core values.

SECTION 2 – OUR PRIVACY PRINCIPLES

Synopsys recognizes that privacy is a human right. We are committed to the following general principles of data privacy and protection. These principles are expressed in our policies and standards and guide our practices:

2.1 No sale of personal information

Synopsys does not sell personal information.

2.2 Purpose limitation

Personal data collected by Synopsys may be used only for the purposes for which it was collected, specified no later than at the time of collection. Except with the consent of the affected individuals, for purposes compatible with their reasonable expectations, or otherwise in line with applicable law, the subsequent processing of the personal information will be limited to these stated purposes.

2.3 Confidentiality

Personal data may be made available only to people with a "need to know" and who have the appropriate clearances.

2.4 Third-party accountability

Synopsys holds third parties with whom personal data is shared to these same privacy principles and standards. Such third parties are required to conduct themselves in a manner consistent with our Code of Ethics and Business Conduct, which includes requirements for the proper handling of personal data, and to execute data processing agreements where applicable.

2.5 Data quality and proportionality

Personal data kept by Synopsys must be accurate, relevant, and not excessive in relation to the purposes for which it was collected.

2.6 Storage limitation

Personal information is to be deleted as soon as it is no longer needed or required to be maintained under applicable laws.

2.7 Transparency

Data subjects are to be informed about how their personal data is used and with whom it may be shared. Synopsys will issue required privacy notices and respond promptly to inquiries about its data processing operations.

2.8 Security

Synopsys will maintain best-practice technical and organizational security measures to protect against such risks as accidental or unlawful destruction, loss, or alteration of personal data, and unauthorized disclosure or access.

2.9 Rights of access, rectification, deletion and objection

In the countries where we do business, Synopsys complies with the requirements of applicable laws, such as the European General Data Protection Regulation (GDPR), that give data subjects the opportunity to be notified about what personal information the Company holds, to verify its accuracy, and in some circumstances to object to the processing of their personal data and demand that it be deleted.

Transparency means enabling individuals to understand and make informed decisions about the processing of their personal information.

2.10 Sensitive data

Synopsys takes additional security measures to protect highly sensitive data (such as medical and health information) in accordance with applicable laws, including the GDPR in Europe and the Health Information Portability and Accessibility Act (HIPAA) in the United States.

2.11 Privacy by design and impact assessments

We consider privacy when building or designing applications, systems and processes that may involve the collection of personal data, and assess them to ensure that privacy-related risks to data subjects are considered and mitigated to the extent reasonably possible.

2.12 Risk and program assessments

Synopsys regularly reviews its privacy program and practices to ensure continued internal compliance, effectiveness and alignment with emerging law and best practices.

2.13 Incident notification

Synopsys will notify affected data subjects promptly after becoming aware of an incident involving a data beach by Synopsys or its vendors as required by law.

2.14 Data used for marketing purposes

Where personal data is used to send sales and marketing communications about Synopsys products, we will follow protocols to ensure that we obtain all required consents, and that we offer opt-out and unsubscribe opportunities as required by applicable laws.

2.15 Putting principles into practice

Synopsys maintains internal policies, protocols, controls and practices that ensure we act consistent with these privacy principles. From our Document Retention Policy, to incident response plans, to new vendor intake procedures, our program spans many processes around Synopsys.

We also provide notices to inform data subject subjects about how their personal data is used and how to invoke their rights. Such notices include the Synopsys Website Privacy Policy and California Consumer Privacy Act Notice posted on our website, workforce privacy notices issued to employees in particular regions, and this Statement. Visitors to our Company website are advised about the ways in which we may collect data (such as the use of cookies) and their options should they prefer not to share their data. We provide recipients of marketing communications with the ability to manage their preferences at any time by accessing our Subscriptions Center.

The Synopsys Integrity Helpline web portal is available to all Synopsys personnel and third parties, 24 hours a day, every day of the year. The Helpline is a dedicated resource for reporting ethics and compliance concerns or suspected violations of the law or our Code of Conduct.

Data subjects who desire more information, or who wish to invoke their rights under applicable privacy laws, are invited to contact privacy@synopsys.com.

SECTION 3 – TO OUR CUSTOMERS

3.1 Global privacy laws

Synopsys was ready for the effective date of the European General Data Protection Regulation (GDPR) in 2018 and the California Consumer Privacy Act (CCPA) in 2020. Under the GDPR, we have an obligation to maintain the security of data concerning European data subjects, respect their rights to access that data and inform them about how data is used, and make sure that in developing applications and systems, we make "privacy by design" and "privacy by default" a part of our culture. Under CCPA we are required to give California consumers similar access to their personal information and establish security measures to prevent data breaches. In addition, Synopsys continues to monitor the development of new data privacy laws in other places where we do business.

3.2 Assisting our customers with compliance

Synopsys is a world leader in application security. Synopsys' security testing tools and services can help our customers comply with the data security requirements of global privacy laws, by establishing reliable measures of risk for their systems and applications and prioritizing remediation efforts to ensure consistent protection of personal data. Synopsys can offer help with:

- Establishing or maturing the customer's software security initiative (SSI)
- Augmenting the security posture of the software the customer uses to process EU resident data
- Tracking and managing vulnerabilities in the open source components in the customer's 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.

3.3 Data protection standards

Maintaining data security means implementing strong data protection standards at Synopsys and passing through rigorous data security requirements to our suppliers. Synopsys' Information Security team is committed to state-of-the-art data protection and cybersecurity. Synopsys has formally adopted the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) to plan, structure, test, and measure our enterprise cybersecurity. Our employees are regularly trained and policies and procedures are assessed regularly by our internal auditors and outside consultants.

We conduct detailed security evaluations of our vendors who handle personal data and other confidential information, and we require our vendors to comply with the Synopsys Information Security Requirements for Vendors.

3.4 Incident response and notification

Synopsys has a detailed company-wide incident response plan designed to allow us to quickly take the steps needed to minimize harm and secure customer data. As required by law, Synopsys will notify affected data subjects promptly after becoming aware of an incident involving a data breach by Synopsys or its suppliers.

3.5 Data controllers, data processors, and GDPR

Under the GDPR, a "data controller" collects and maintains personal data and decides how it is to be processed. A "data processor" follows the instructions of the data controller for processing personal data. In connection with the products and services it provides, Synopsys does not typically process personal data on its customers' behalf. When we use customer employee contact information to complete orders, conduct business, or enable logins (where user names and passwords are hashed), it's more accurate to say that Synopsys acts as a data controller.

In those rare cases where Synopsys does act as a data processor on behalf of a customer, Synopsys will enter into an appropriate form of data processing agreement in which Synopsys will agree to:

- process personal data only on the written instructions of the controller;
- take all measures required pursuant to article 32 of the GDPR in respect of the personal data;
- ensure that its staff who are authorized to process the personal data have committed themselves to confidentiality;
- ensure that its subcontractors who process such personal data are in turn subject to obligations substantially identical to those applicable to Synopsys;
- at the customer's cost, assist the customer through appropriate technical and organizational measures (insofar as possible) to respond to a request by a data subject to exercise his or her rights in respect of the personal data;
- not transfer such personal data onward to recipients outside of GDPR jurisdictions without adequate safeguards;
- at the customer's cost, make available to the customer all information necessary to demonstrate Synopsys' compliance with these obligations; and
- promptly notify the customer of requests received directly from data subjects with respect to personal data submitted through the Synopsys products or services.

3.6 Personal information and CCPA

Under the CCPA, a company that utilizes a service provider to process personal information of California consumers on its behalf must enter into a written agreement prohibiting the service provider from selling the personal information or using the information for any purpose other than performing the services specified in the contract.

Again, Synopsys does not generally process personal information on behalf of our customers, and Synopsys does not sell personal information. In an appropriate situation Synopsys will enter into agreements acknowledging that as a third party, Synopsys is prohibited from (a) selling any personal information of its customers or their employees, (b) retaining, using or disclosing the personal information for any purpose other than performing the services described in the applicable contract, and (c) retaining, using or disclosing the personal information outside of the direct business relationship between the customer and Synopsys.

Data Security means implementing strong data protection standards at Synopsys and passing through rigorous data security requirements to our suppliers.

SECTION 4 – TO OUR WORKFORCE

4.1 A global workforce

Synopsys has employees and contractors all over the world. We need to be able to transfer information across national borders in order to operate our business, including recruiting the best talent, providing them with pay and benefits, evaluating and counseling them regarding their performance, and sharing information about their opportunities for community involvement. In so doing, we are mindful of the laws in each country where we work, particularly those that pertain to data privacy and protection.

Synopsys maintains effective controls on who may access the personal data of our workforce as well as policies regarding how data is to be retained, and for how long.

4.2 GDPR compliance

For members of our workforce who live in Europe, the GDPR (mentioned in Section 3.1 above) imposes special requirements. Synopsys GDPR-compliant practices include, but are not limited to:

- Robust policies and notices to reflect current laws and advise data subjects of their rights under the GDPR
- GDPR-compliant data processing agreements with the outside companies that process employee data on Synopsys' behalf
- Document retention policies under which we do not maintain personal data any longer than required in order to fulfill our legal obligations
- Data privacy training as part of our regular Ethics and Compliance Training, which must be completed by every Synopsys employee, as well as specialized training for groups who access and use personal data within Synopsys.
- Inter-company agreements between the US parent company and its European subsidiaries to enable the lawful transfer of personal data between Europe and the United States. (We rely on the Standard Contractual Clauses approved by the European Commission for this purpose. Synopsys had never relied on the invalidated Privacy Shield framework.)

Employees who desire more information, or who wish to invoke their data subject rights, are invited to contact privacy@synopsys.com.

4.3 Keeping data safe

Our commitment to data security extends to protecting personal data as well as Synopsys' intellectual property from theft. This includes the use of badged access, video monitoring, and the like to maintain physical security, as well as firewalls, encryption, and data loss prevention measures to prevent the misuse of Synopsys' systems and devices. We obey applicable privacy laws whenever we monitor the use of Synopsys-owned systems and devices.

SYNOPSYS®

SECTION 5 – TO OUR VENDORS AND SUPPLIERS

5.1 A valued partnership

Synopsys values the many vendors and suppliers who provide us with tools to help us manage information about our workforce, our customers, and others.

5.2 Our code of conduct

Synopsys looks to its vendors to conduct business consistent with our Code of Ethics and Business Conduct, which includes data privacy and protection requirements as well as other obligations to ensure that we do business the right way. Put simply, we do business the right way when we act ethically and consistently with our core value of integrity. We look forward to partnering with other organizations in pursuit of this goal.

To protect the integrity of personal data and other sensitive information, we also require all our vendors to comply with the Synopsys Information Security Requirements for Vendors.

5.3 Data processing agreements

Under the GDPR (mentioned in Section 3.1), Synopsys is required to have appropriate agreements in place with each vendor who handles the personal data of European data subjects. Any business involved in the processing of personal data of a European data subject must comply with the GDPR, regardless of where the processor's business is located.

Accordingly, we require many vendors and suppliers to sign data processing agreements (DPAs). This is necessary to ensure proper handling and protection of employee and customer data and to provide a valid legal basis for transfers of personal data from Europe to the US. We have found that most of our vendors are already aware of these requirements, which are as important for their own compliance with the GDPR as for ours.

SECTION 6 – MORE INFORMATION

We invite anyone who desires more information about Synopsys' practices and compliance with data privacy laws to contact any of the following: the Synopsys Data Privacy Officer, if one has been designated in the country where you reside, the Company's Chief Privacy Officer at privacy@synopsys.com, the Chief Ethics and Compliance Officer at ethics.officer@synopsys.com, or the Synopsys Legal Department.

This Statement was last revised March 10, 2021

SYNOPSYS®