

Oracle Products and Services and the EU Cyber Resilience Act

Regulation (EU) 2024/2847 the European Cyber Resilience Act (the “CRA”) sets out cybersecurity requirements and vulnerability handling and management obligations for products with digital elements made available on the EU market. The CRA entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027, with reporting obligations to apply as of 11 September 2026.

The CRA establishes horizontal cybersecurity requirements for products with digital elements, including hardware and software, made available on the EU market. It aims to ensure that such products are designed, developed, and maintained with security throughout their lifecycle.

Oracle aligns with its obligations under the CRA, and will continue to offer in-scope products and services with industry-leading security controls and product security standards designed to support applicable CRA requirements. These include: cybersecurity measures, secure product development, vulnerability handling and management, and security incident response.

As implementation guidance and supporting standards continue to evolve, Oracle will continue to assess the applicable CRA requirements and provide information to help customers understand Oracle’s approach to the CRA and relevant product security capabilities.

We hereby invite you to review Oracle’s security policies and additional resources¹ that may apply to the Oracle products and services you have purchased or consider purchasing. If you have further questions about this statement or about Oracle’s security policies, please consult your Oracle sales representative.

Copyright © 2026, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

¹ To learn more about Oracle’s industry standard security and incident response practices, see; [Oracle Corporate Security Practices](#); [Oracle Software Security Assurance \(OSSA\)](#); [Oracle Security Incident Response](#); [Oracle Secure Coding Standards \(SCS\)](#)