



# Oracle Cloud Services and the NIS2 Directive

As part of the EU Cybersecurity strategy, Directive 2022/2555/EC (the “**NIS2 Directive**”) came into force on January 16, 2023, replacing and repealing Directive 2016/1148/EC (the “**NIS1 Directive**”) and requires adoption into EU Member State law.<sup>1</sup> This statement provides information on how Oracle supports its customers in complying with these legislative developments.

The NIS2 Directive aims to improve cybersecurity risk management processes across the EU by addressing deficiencies in previous NIS 1 requirements and expanding the scope to cover more sectors.

Similar to its predecessor, it requires essential and important entities to implement appropriate technical and organizational measures to manage cybersecurity risks to their network and information systems. It also sets out mandatory reporting obligations, requiring companies to notify the relevant cybersecurity authorities about incidents that significantly impact the continuity of their services.

Oracle understands that its customers operating as essential or important entities need to manage their security practices carefully in line with the updated NIS2 Directive cybersecurity requirements. These requirements are not new to us and we will continue to offer our Cloud services with industry leading security controls. These controls are embedded in our Cloud services and Cloud data centers in every major region around the world, including the EU.

We therefore invite you to review our [NIS2 Advisory](#), security policies and additional resources<sup>2</sup> that may apply to the Cloud service offerings you have purchased or consider purchasing from Oracle.

Oracle will also continue to monitor developments around the NIS2 Directive, such as the EU member states implementation process and guidance issued by national regulators. If you have further questions about this document or about Oracle’s security policies, please consult your Oracle Cloud sales representative.

Copyright © 2025, 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.

---

<sup>1</sup> See European Commissions Policy Page for the latest status of transposition process of EU Member states: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

<sup>2</sup> To learn about attestations available for various cloud services, see [Oracle Cloud Compliance Dashboard](#) and to review Oracle’s industry standard cloud security assessments, see [Oracle Cloud Security Practices](#).