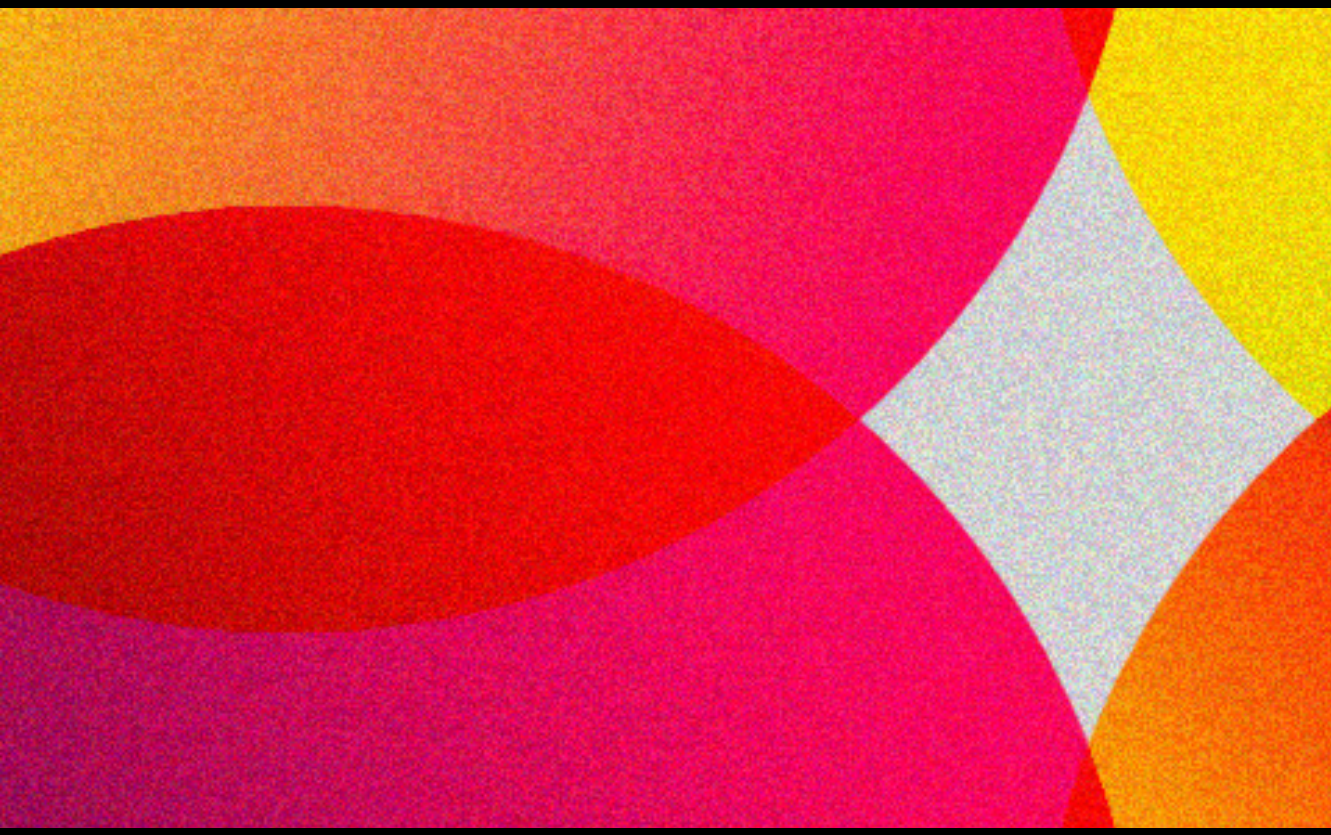
KONTENT.AI®



Kontent.ai provides NIS 2 compliance for customers

www.kontent.ai

Kontent.ai is committed to maintaining confidentiality, integrity, and availability of data that customers entrust into our product. To help assure our European customers of the high standards we put into the protection of their data and the cyber resilience of our product offering, we have prepared this whitepaper that explains how Kontent.ai addresses the requirements of the NIS 2 Directive.

Executive summary

Kontent.ai application has been developed with security and privacy in mind. It contains security features that help customers protect their data. In addition, the internal operation of Kontent.ai as an organization follows industry standards and best practices to ensure that customer data remains secure.

- Kontent.ai has a strong emphasis on security, coordinated by the internal security team led by CISO
- The security program of Kontent.ai is focused on protecting customer data and covers all areas of application, infrastructure, information, physical, and supply chain security
- As an assurance, ISO/IEC 27001, 27017, and SOC 2 Type 2 certifications/audit reports are provided to customers upon a request

How to work with this material

Kontent.ai has prepared this whitepaper to inform customers about:

- How Kontent.ai addresses the specific NIS 2 Directive requirements internally
- What further steps can customers take to increase security when using Kontent.ai application

These elements comprise a shared responsibility model in Kontent.ai cloud offering. The attached table (see below) can be read by rows, where every row covers a specific requirement, Kontent.ai internal operation, and further recommendations. It is essential to review those recommendations and utilize all security features and functions of Kontent.ai application. Note that not all member state laws were taken into consideration, and there may be changes in interpretation for companies operating in certain European regions.

The table covers merely relevant requirements we have chosen to demonstrate compliance and is not an exhaustive list. Customers are encouraged to contact Kontent.ai through their customer representative or security@kontent.ai should they seek further answers.

Overview of the shared responsibilities

NIS 2 Requirement	Description	Kontent.ai's Internal Measures	Customer Actions for Enhanced Security
Article 20	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of network and information systems that those entities use for their operations or the provision of their services and to prevent or minimize the impact of incidents on recipients of their services and other services.	The Security Program of Kontent.ai is based on risk management and a risk-based approach. There is a range of security controls in place for the protection of the product environment and customer data.	Ensure best practices to configure Kontent.ai application, including activating security features and managing authentication and authorization in a secure manner
Article 21 2. (a)	policies on risk analysis and information system security;	Kontent.ai has put in place all necessary and relevant policies for Information Security, in line with ISO/IEC 27001, 27017 requirements and NIST recommendations.	Request policy samples from the customer representative or directly access them via the Kontent.ai Trust Center.
Article 21 2. (b)	incident handling;	Kontent.ai has established internal procedures for incident reporting and response. Our Security Steering Committee oversees this process.	Customers should report any security incidents related to Kontent.ai to our Security Team via security@kontent.ai. All security events and status of Kontent.ai application can be traced online via https://status.kontent.ai

NIS 2 Requirement	Description	Kontent.ai's Internal Measures	Customer Actions for Enhanced Security
Article 21 2. (c)	business continuity, such as backup management and disaster recovery, and crisis management;	Business continuity and disaster recovery processes are put in place and tested on a regular basis. For more information on backup, refer to this page	If customers seek to back up their data outside of Kontent.ai application, it is possible. Refer to this page for more information.
Article 21 2. (d)	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Kontent.ai assesses its suppliers and partners for security compliance. We maintain a Software Bill of Materials (SBOM) for transparency.	Customers can subscribe to Kontent.ai SBOM data via security@kontent.ai. Trust Center of Kontent.ai can be accessed to review the latest certifications, attestations, audits, and penetration testing reports.
Article 21 2. (e)	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Kontent.ai addresses the security of new infrastructure or system components through a process involving due diligence, security architecture assessment, threat modeling, and secure implementation practices resulting in the secure operation of the system/component, including lifetime handling of vulnerabilities and hardening.	Customers are advised to review security architecture when integrating the Kontent.ai application into their workflow and encouraged to utilize security features and configurations of the Kontent.ai application.

NIS 2 Requirement	Description	Kontent.ai's Internal Measures	Customer Actions for Enhanced Security
Article 21 2. (f)	policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Kontent.ai executes internal and external security audits, vulnerability assessments, penetration tests and other tests and reviews according to the annual Audit Plan.	Customers are welcome to review results from penetration tests, self-assessment questionnaires, SOC 2 Type 2 Audit Reports, and Bridge Letters via the Kontent.ai Trust Center.
Article 21 2. (g)	basic cyber hygiene practices and cybersecurity training;	Kontent.ai Security Awareness Training program consists of policy awareness, role-based training, secure practices for users, secure development and coding training, and simulated phishing exercises. On-the-job training is provided as well, and we utilize gamifications where appropriate.	We recommend training users of Kontent.ai applications on best practices. Certification paths for various roles, including security topics, are available via Kontent.ai Learn.
Article 21 2. (h)	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Kontent.ai ensures data encryption in transit and at rest. We follow industry best practices for encryption. For more information, refer to this page.	-

NIS 2 Requirement	Description	Kontent.ai's Internal Measures	Customer Actions for Enhanced Security
Article 21 2. (i)	human resources security, access control policies, and asset management;	Kontent.ai enforces strict access controls, role-based permissions, and multi-factor authentication (MFA) for both Kontent.ai application and our internal infrastructure. There are controls in place to address security in human resources, in line with ISO/IEC 27001 requirements.	Customers should configure access controls appropriately within their Kontent.ai accounts and encourage MFA usage. For more information, refer to this page.
Article 21 2. (j)	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Kontent.ai utilizes multi-factor authentication in the internal environment and risk-based conditional access policies in line with Zero Trust architecture.	Customers are recommended to utilize multi-factor authentication, either using their identity provider or Kontent.ai application. For more information, refer to this page.
Article 23	Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident)	Kontent.ai follows legal requirements for incident reporting and, in case such a situation happens, informs relevant authorities and/or customers within the legally required limits.	All security events and status of Kontent.ai application can be further traced online via https://status.kontent.ai

Information in this whitepaper is for informational purposes only and does not constitute legal advice. It discusses how Kontent.ai helps comply with key requirements from the NIS 2 Directive. The information provided is based on general principles of European Union laws and regulations as of the publication date. The information provided in this Whitepaper may not reflect local member state laws, recent changes in NIS 2 regulations, or legal interpretations. Readers are advised to consult legal professionals for tailored advice and guidance. **While efforts have been made to ensure accuracy, no representation or warranty, express or implied, is made regarding completeness, accuracy, reliability, or suitability. Kontent.ai is not liable for any direct, indirect, incidental, consequential, punitive, or special damages arising out of or in connection with the use of this Whitepaper or reliance on the information contained herein**. Customers are responsible for their own compliance with NIS 2 and any other regulations and for ensuring that Kontent.ai application is used in compliance with applicable laws.

About Kontent.ai

Kontent.ai's mission is to help the world's leading organizations achieve an unparalleled return on their content. In the industry's first AI-powered CMS, content teams plan, create, and optimize content and deliver it to any channel—quickly, securely, and flexibly. Kontent.ai is designed to support organizations with exacting governance requirements, often in highly regulated industries and with complex content value chains.

Tight permissions control all operations; enterprise-grade security and privacy keep content safe. With a demonstrated ROI of 320%, Kontent.ai customers, including PPG, Elanco, Zurich Insurance, Cadbury, and Oxford University, benefit from a measurable step change in how their teams operate, increasing content velocity, mitigating risk, and maximizing yield. Kontent.ai is a Microsoft partner, MACH Alliance member, and recognized vendor by Gartner and Forrester. Learn more at: kontent.ai.

Want to see Kontent.ai in action?

Schedule a demo

KONTENT.AI®