Kontent.ai

Kontent.ai complies with DORA.

The Digital Operational Resilience Act (DORA) is an EU regulation that aims to enhance the digital operational resilience of the financial sector by introducing consistent rules on ICT risk management, incident reporting, testing, and oversight of ICT third-party serv ice providers. DORA applies to a wide range of financial entities in the EU. It is expected to be fully implemented by January 2025.

Kontent.ai is a headless content management system (CMS) that enables organizations to achieve an unparalleled return on their content and engage meaningfully with their customers. Kontent.ai allows you to manage content in one place and deliver it to any front-end or UI. You can reuse and remix content across various multimedia and digital channels without duplication overheads. Kontent.ai is an efficient and cost-effective solution for managing content.

Kontent.ai helps you comply with DORA requirements and demonstrate your digital operational resilience in the areas of:

- ICT risk management and governance
- ICT-related incident management
- Resilience testing
- Third-party risk management
- Information sharing

ICT risk management and governance.

DORA requires financial entities to establish and implement an ICT risk management framework that covers the identification, assessment, mitigation, monitoring, and reporting of ICT risks. The framework should also include policies, procedures, processes, tools, systems, and controls to ensure the confidentiality, integrity, availability, and authenticity of data and systems.

Kontent.ai has a robust framework in place that covers Governance, Risk, and Compliance. For risk management, there is a Risk Appetite Statement approved by top management, and the ongoing risk assessment classifies risks using risk quantification. To satisfy requirements of Article 5, 2 i), Kontent.ai informs customers of upcoming major changes proactively.

Kontent.ai further helps you reduce risks by providing you with a secure, reliable, and scalable cloud-based headless CMS platform. Kontent.ai offers the following features for the protection of confidentiality, integrity, and availability:

- **Encryption**: Kontent.ai encrypts data at rest and in transit using industry-standard algorithms and protocols. You can also use your own encryption keys to protect your sensitive data.
- **Authentication**: Kontent.ai supports various authentication methods, such as email/password, single sign-on (SSO), social login, and API keys. You can also integrate with your own identity provider (IdP) using OpenID Connect or SAML 2.0 protocols.
- **Authorization**: Kontent.ai allows you to define granular permissions and roles for your users and collaborators. You can also use custom policies to enforce specific rules and conditions for accessing your content.
- **Audit logs**: Kontent.ai records all actions performed by users and API calls in audit logs. You can access the audit logs via the web app or the API. You can also export the audit logs to your own storage or analytics service.

- **Backup and restore**: Kontent.ai automatically backs up your data every day and keeps it for 30 days. You can also create manual backups anytime you want. You can restore your data from any backup point in case of data loss or corruption.
- **Compliance**: Kontent.ai complies with various industry standards and regulations, such as GDPR, ISO 27001, HIPAA, SOC 2 Type II, and more. You can find more information about our compliance certifications on Kontent.ai website.
- **Technological resilience**: Kontent.ai provides protection against Denial of Service attacks. This is included in all plans.

ICT-related incident management.

DORA requires financial entities to establish and implement a management process to monitor and log ICT and cyber-related incidents.

Kontent.ai helps you respond to and report ICT incidents by providing you with monitoring and support during all stages of incident management. Kontent.ai offers the following features and benefits for incident response and reporting:

- **Monitoring**: Kontent.ai monitors the performance, availability, reliability, and security of its platform using various tools and metrics. You can also monitor your own content delivery or management using our Sync API together with webhooks.
- **Incident support**: Kontent.ai has its own incident management process following NIST SP 800-61 and ISO/IEC 27001 standards. In case of customer investigation, Security and Support Teams assist customers with data and further insights as needed.
- **Incident reporting**: Kontent.ai reports incidents to the relevant authorities as required by law. Such practices are often further discussed in the agreements with customers.

Digital operational resilience testing.

DORA requires financial entities to periodically test their capabilities and functions included in the ICT risk management framework for preparedness and identification of weaknesses, deficiencies, or gaps, as well as the prompt implementation of corrective measures.
The regulation allows for a proportionate application of digital operational resilience testing requirements depending on the size, business, and risk profiles of financial entities.

Kontent.ai supports the resilience testing of financial entities with its own set of tests conducted on a regular basis, as well as enabling customer tests:

- **Regular security tests**: Kontent.ai performs a variety of security tests for both the product and the underlying infrastructure. These include ongoing vulnerability assessments, security audits, and annual full OWASP penetration tests. A collection of in-house, external, and commercial tools are utilized for vulnerability scanning. There are ongoing tests running for each new version of Kontent.ai application to ensure the security of product increments.
- **Vulnerability disclosure program**: Kontent.ai operates the Vulnerability Disclosure Program, which rewards security researchers with bug bounties or recognition for their findings.
- **Disaster recovery testing**: On at least an annual basis, Kontent.ai conducts full recovery tests, covering various disaster scenarios and simulated recovery.
- **Customer audits and penetration tests**: Customers are welcome to perform their own audits or penetration tests as long as they comply with Kontent.ai terms and conditions of their plan as well as the Penetration Testing Policy. Customer Success Managers are dedicated to helping set up such testing if needed.

Third-party risk management.

DORA requires financial entities to monitor third-party risk providers and ensure that they comply with the same ICT risk management standards as the financial entities themselves. The regulation also introduces key contractual provisions that must be included in the agreements between financial entities and third-party providers. Furthermore, the regulation establishes an oversight framework for critical ICT third-party providers based on criteria such as market share, number of clients, systemic importance, etc.

Kontent.ai helps you manage your risks by providing you with a transparent, accountable, and compliant platform that integrates seamlessly with your existing systems and tools. Kontent.ai supports the third-party risk management of financial entities in the following ways:

- **Security standards**: Kontent.ai adheres to a range of security certification frameworks, including ISO/IEC 27001, 27017, Trusted Services Criteria (compliance can be demonstrated by SOC 2 Type 2 Report), and Cloud Control Matrix (as discussed in CAIQ). Apart from those, various other standards are used internally to measure and increase process and control maturity, including NIST frameworks, CIS benchmarks, or OWASP standards.
- **Contractual provisions**: Kontent.ai is prepared to support contractual provisions required by DORA for third-party providers. As defined in DORA, these include service level agreements (SLAs), data protection clauses, audit rights, incident notification obligations, termination rights, etc.

Information sharing.

DORA encourages financial entities to exchange information and intelligence on cyber threats with other financial entities and authorities in order to enhance their collective digital operational resilience. The regulation also provides legal certainty and protection for financial entities that share such information in good faith.

Kontent.ai shares important security-related information by the following means:

- **Service status**: Any events affecting Kontent.ai application are shared via status.kontent.ai. The changelog can be found at Product updates | Kontent.ai Learn.

Software Bill of Materials: Kontent.ai shares its Software Bill of Materials (SBOM) upon request. Customers can request a subscription through their customer representative or contact us via security@kontent.ai.

Conclusion.

DORA is an EU regulation that aims to enhance the digital operational resilience of the financial sector by introducing consistent rules on ICT risk management, incident reporting, testing, and oversight of ICT third-party service providers. DORA applies to a wide range of financial entities. It is expected to be fully implemented by January 2025.

Kontent.ai is a headless CMS that enables organizations to achieve an unparalleled return on their content and engage meaningfully with their customers. Kontent.ai allows you to manage content in one place and deliver it to any client application. You can reuse and remix content across various multimedia and digital channels without duplication overheads. Kontent.ai is a more efficient and cost-effective solution for managing content.

Kontent.ai helps you comply with DORA requirements and demonstrate your digital operational resilience. Kontent.ai provides you with a secure, reliable, scalable, flexible, adaptable, transparent, accountable, and compliant platform that integrates seamlessly with your existing systems and tools. Kontent.ai supports various features and benefits for ICT risk management and governance, incident response and reporting, resilience testing, third-party risk management, and information sharing.

If you want to learn more about how Kontent.ai can help you comply with DORA and achieve digital operational resilience, please visit our website or contact us.

Information in this whitepaper is for informational purposes only and does not constitute legal advice. It discusses how Kontent.ai helps with compliance with key requirements from the Digital Operational Resilience Act (DORA). The information provided is based on general principles of European Union law and regulations as of the publication date. The information provided in this Whitepaper may not reflect recent changes in DORA regulation 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 DORA and any other regulations and for ensuring that Kontent.ai application is used in compliance with applicable laws.*

Kontent.ai

About Kontent.ai.

Kontent.ai is the headless CMS that enables organizations to have complete control over content to speed up time to market and engage meaningfully with audiences across channels.

With offices in New York, London, Amsterdam, Brno, and Sydney, Kontent.ai supports global customers including Zurich Insurance, Algolia, and Oxford University. Kontent.ai is a Microsoft partner and MACH Alliance member, recognized by both Gartner and Forrester. Visit kontent.ai to learn more about how we empower leading organizations.

SCHEDULE YOUR DEMO →