Kontent.ai

Kontent.ai provides GLBA compliance for customers.

Kontent.ai is committed to maintaining confidentiality, integrity, and availability of data that customers entrust into our product. To help ensure our financial customers of the high standards we put into the protection of customer information, we have prepared this whitepaper that explains how Kontent.ai addresses the requirements of Standards for Safeguarding Customer Information as part of the Gramm-Leach-Bliley Act.

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, including customer information under GLBA, remains secure.

- The Kontent.ai application supports use cases that require sensitive data (including, e.g., protected health information under HIPAA)
- 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 requirements internally
- What further steps can customers take to secure customer information under GLBA when using Kontent.ai application

These elements comprise a shared responsibility model over customer information under GLBA in the cloud environment. The attached table 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 in order to protect customer information.

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.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.3	Information security program	Kontent.ai has a formal Information Security Program in place that covers all customer data and related infrastructure. This does not substitute but can support customers' Security Programs.	–
§314.4 (a)	Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, “Qualified Individual”).	There is a Chief Information Security Officer who leads the Security Team at Kontent.ai. Even though this does not substitute for Qualified Individuals that the financial institution needs to designate, the Kontent.ai Security Team can assist Qualified Individuals in matters regarding Kontent.ai controls.	Qualified Individuals are welcome to engage with the Kontent.ai Security Team.
§314.4 (b)	Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.	The Program of Kontent.ai is also based on risk management as one of the main pillars for implementing appropriate measures to protect customer data and related infrastructure. It is performed on a continuous basis, with a major review done at least annually or when an important business change occurs. Kontent.ai has defined and approved the Risk Appetite Statement and works with quantifiable methods to calculate the potential loss.	Customers are advised to consider Kontent.ai application in their risk assessment if it is used to process customer information under GLBA. Internal controls of Kontent.ai can be reviewed e.g. via SOC 2 Type 2 report that can be shared as needed. Security features of Kontent.ai can be utilized to support maintaining the security, confidentiality, and integrity of customer information.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (c) (1)	Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to: (i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and (ii) Limit authorized users' access only to customer information that they need to perform their duties and functions or, in the case of customers, to access their own information;	(i) Kontent.ai has implemented processes to ensure only authorized individuals gain access to important assets, including customer data and infrastructure. These include background checks, onboarding, training, access reviews, and management on a regular basis or during a change of assignment or termination. (ii) There are strict rules governing access to any customer data. The access is utilized only in disaster and in support cases based on the customer's designation and approval.	(i) Kontent.ai recommends only granting access to the application to authorized individuals and regularly checking if they are still necessary. To ensure the confidentiality of data during the whole content lifecycle, it is possible to restrict access to the published content. https://kontent.ai/learn/tutorials/develop-apps/build-strong-foundation/restrict-public-access/ Customers should consider using customizable expiration times for API keys to manage the security of their integrations. (ii) The roles and permissions in Kontent.ai can be set up in a granularity that reflects the customer's needs. Kontent.ai recommends following the least privilege principle when designing the permission model in Kontent.ai application. For more information, see https://kontent.ai/learn/tutorials/set-up-kontent-ai/set-up-team-and-collaborate/roles/. Furthermore, taxonomies (https://kontent.ai/learn/tutorials/manage-kontent-ai/taxonomies/model-taxonomies-right/) and/or content groups (https://kontent.ai/learn/tutorials/manage-kontent-ai/content-modeling/organize-elements-with-content-groups/) can be used for organizing content so that customer information under GLBA is clearly distinguished in the system.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (c) (2)	Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;	Kontent.ai performs asset identification, classification, and management according to the internal policies.	Customers should keep an overview of the assets they process in Kontent.ai applications. Taxonomies and content groups can help organize and classify the content.
§314.4 (c) (3)	Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;	Customer data processed by Kontent.ai is encrypted both at rest and in transit. More information can be found in Kontent.ai Learn: https://kontent.ai/learn/tutorials/references/data-encryption/	Customers are required to use browsers and workstations in versions that support the used cryptographic protocols.
§314.4 (c) (4)	Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;	Kontent.ai utilizes the Secure Software Development Lifecycle for the development. More information can be found at: https://kontent.ai/blog/kontent-ai-sdlc-in-agile-methodology/ As for testing the security of Kontent.ai application, the most recent penetration testing reports, SOC 2 Type 2 Report, and ISO certificates are provided to customers upon request.	Customers are welcome to perform penetration testing of the platform as long as they comply with Penetration Testing Policy. All cases should be requested via security@kontent.ai.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (c) (5)	Implement multi-factor authentication for any individual accessing any information system unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;	For internal systems, Kontent.ai enforces multi-factor authentication for all access to all relevant systems or data.	Kontent.ai application can be configured to enforce multi-factor authentication for users. This is available for Enterprise plans. For more information, refer to https://kontent.ai/learn/docs/security/multifactor-authentication. When using Single Sign On, the customer's authentication provider may provide this functionality instead.
§314.4 (c) (6)	(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and (ii) Periodically review your data retention policy to minimize the unnecessary retention of data;	—	(i) Data in Kontent.ai application can be disposed of according to the needs of the particular retention policy. This is managed by the customers themselves. Note that there is up to 90-day window (due to how backups operate) after deleting the data before they are completely deleted. (ii) Kontent.ai recommends reviewing data retention policies and practices to delete the data in Kontent.ai application on a regular basis.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (c) (7)	Adopt procedures for change management	There are internal change and configuration management procedures defined in Kontent.ai policies and applicable for relevant product and infrastructure changes.	For the changes of content items in the Kontent.ai application, customers are advised to utilize item workflows. Refer to: https://kontent.ai/learn/docs/workflows-publishing/change-item-workflow
§314.4 (c) (8)	Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.	The activity of authorized users is logged. There are records in place about access to customer data. All this activity is captured in internal Kontent.ai policies with defined roles, responsibilities, and procedures.	Through the Audit Log feature of Kontent.ai application, customers may access a journal containing all changes to content types, snippets, and asset types. Refer to: https://kontent.ai/learn/docs/security/audit-log
§314.4 (d) (1)	Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on or intrusions into information systems.	Kontent.ai performs regular security reviews, audits, and penetration tests to ensure ongoing assurance for customers.	Customers are advised to perform regular reviews of Kontent.ai application, including but not limited to access rights, roles, permissions, audit logs, content, and uploaded files.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (d) (2)	For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct: (i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and (ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.	Kontent.ai performs both internal and external evaluations of security, including audits, reviews, vulnerability assessments (on an ongoing basis), and penetration tests (at least annually).	For their own audit needs, customers may request the latest copies of penetration testing done on Kontent.ai application, as well as SOC 2 Type 2 report or security certificates. These are shared under an NDA. Furthermore, customers are advised to monitor or subscribe to updates on incidents and outages of Kontent.ai application via https://status.kontent.ai

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (e) (1)	Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;	There is a comprehensive security culture program that comprises security awareness trainings, tests, gamification, recognitions, and more.	It is recommended to provide additional training for relevant roles responsible for securing and working with customer information under GLBA within Kontent.ai application. Refer to Kontent.ai Learn for relevant training and documentation on security features: https://kontent.ai/learn/
§314.4 (e) (2)	Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;	The Security Team in Kontent.ai is led by CISO and utilizes qualified individuals with experience in various industries, including highly regulated environments.	—
§314.4 (e) (3)	Providing information security personnel with security updates and training sufficient to address relevant security risks;	The individuals in the Security Team undergo regular training and are holders of various certifications and credentials from ISACA, ISC(2), PECB, The Open Group, Microsoft, and others, as well as advanced cyber security degrees.	—
§314.4 (e) (4)	Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.	There is a personalized development plan for each individual in the Security Team of Kontent.ai that covers both individual needs and development in the security field, including new threats and measures.	Customers are advised to subscribe their security teams to https://status.kontent.ai to receive information about incidents and outages.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (f) (1)	Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;	There is a formal process for supply chain risk management in Kontent.ai. When selecting new suppliers, provided safeguards and assurance are compared with the asset classification and the level of risk.	For due diligence on Kontent.ai, customers are encouraged to review all relevant information provided on the Kontent.ai website and materials shared with the customer representative. ISO/IEC 27001, 27017 certificates with Statement of Applicability, SOC 2 Type 2 Report, recent penetration testing report, and whitepapers on compliance are provided upon request. CAIQ can be downloaded directly from the website of Cloud Security Alliance https://cloudsecurityalliance.org/star/registry/kontent-ai/services/kontent-ai/. Learn Articles contain technical references about security features in the Kontent.ai application https://kontent.ai/learn/docs/security. Kontent.ai blog contains various resources on security https://kontent.ai/blog/
§314.4 (f) (2)	Requiring your service providers by contract to implement and maintain such safeguards;	There are contracts defining security, confidentiality, and privacy requirements in place with relevant suppliers of Kontent.ai.	Security and privacy safeguards are part of the contractual documentation with Kontent.ai.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (f) (3)	Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.	Kontent.ai reviews their suppliers based on the level of their classification on a regular basis.	SOC 2 Type 2 Report and penetration testing report, along with the most recent certifications, can be provided regularly, upon request.
§314.4 (g)	Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.	A regular management review of the Information Security Program, measurement and monitoring, and internal and external audits are in place to ensure the ongoing relevance of controls in place.	Customers are advised to utilize new security features of Kontent.ai application as they come live. Contact through customer success management can ensure further improvements of relevant security controls.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (h)	Establish a written incident response plan designed to promptly respond to and recover from any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas: (1) The goals of the incident response plan; (2) The internal processes for responding to a security event; (3) The definition of clear roles, responsibilities, and levels of decision-making authority; (4) External and internal communications and information sharing; (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (6) Documentation and reporting regarding security events and related incident response activities; and (7) The evaluation and revision as necessary of the incident response plan following a security event.	Kontent.ai utilizes complex processes for security incident management. Incidents are managed by their severity, triaged, documented, and communicated. The process follows NIST recommendations and the ISO 27001 framework.	In case of a security incident concerning Kontent.ai application or customer information there, customers are advised to contact the support without undue delay.

Paragraph	Safeguards	Kontent.ai Controls and comments	Kontent.ai Recommendations
§314.4 (i)	Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information: (1) The overall status of the information security program and your compliance with this part; and (2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.	There are quarterly reviews of the security program and the Security Steering Committee meetings that ensure oversight over Security Program of Kontent.ai.	–

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 Standards for Safeguarding Customer Information. The information provided is based on general principles of United States law and regulations as of the publication date. The information provided in this Whitepaper may not reflect recent changes in GLBA 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 GLBA and any other regulations and for ensuring that Kontent.ai application is used in compliance with applicable laws.

Kontent.

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 →