Engagement Made Easy®

AI Charter

Prepared by:	Information Security department
Date Issued:	15 September 2025
Version:	1.0 (full release version)
Classification:	**Public**
File Reference:	AI Security Posture 2025 - Version 1.0

Purpose of this document

Content Guru (CG) is an award-winning organisation providing voice and data platform solutions globally. With the advent of AI technologies and the introduction of relevant worldwide regulation, Content Guru has set out this Charter to state how it manages and utilises AI.

This document sets out our key principles and frameworks that have also been woven into our core corporate policy sets and is designed to enable the reader to understand CGs approach to AI.

This Charter is applicable and is an umbrella Charter for all parts of CG, its products, services and business partners, be they for internal or external customer (e.g., product) use.

Where legal frameworks are referenced e.g., the EU AI Act 2024 (Regulation (EU) 2024/1689), Content Guru develops, supports and abides by local legislations in all cases; therefore, use of Content Guru customer products and services not in adherence to local legislations is soley at the liability of the users/customer organisations.

For the avoidance of doubt, in line with the Act, Content Guru as the provider of customer solutions and systems, is classed as a '**provider**'.

How our technology works

Content Guru provide multiple voice & data platform solutions and applications based on its award-winning **storm®** environment. Within these solutions are AI based technologies services provided both by Content Guru and its third-party business partners (such as Microsoft & Speechmatics), in these cloud solutions.

These solutions receive the media stream and utilise the AI platforms to support in real time back to **storm**, an example here is the Real Time Text translation service, where it's presented in the DTA as the agent takes the call. The transcription captures both agent and customer speech, displaying them in separate speech text bubbles and this can be copied by the agent directly from DTA into any system of record using the provided copy button. If an organisation has chosen to not save a history of the transcription, on completion of call wrap up the data is purged, and the agent is made ready for the next call. Data is only stored in line with the standard data processing agreement, regulatory requirements and contractual agreements.

The **storm** service is designed to ensure secure and auditable segregated services for all customers. This is achieved through a multi-tenanted cloud-delivered service model, where each customer's services run in a secure, partitioned environment using the concept of 'organisations'. All applications, workflows, and data interconnects are provisioned per organisation. This separation is maintained through the use of multi-factor authenticated logins (e.g., RSA SecurID), ensuring that each organisation's data, configuration, and capabilities are inaccessible to others.

Content Guru has introduced AI in line with industry and regulatory needs e.g., the EU AI Act AI policies and standards for development and running of its solutions and platforms, both for its customers and employees

Content Guru products & services

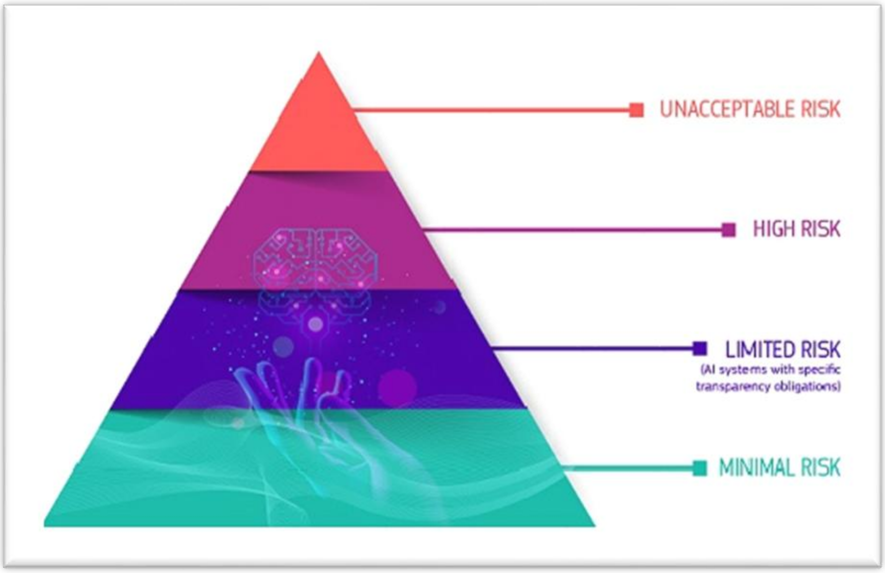
Content Guru is defined as a ‘provider’ within the Act.

Content Guru provides AI systems which could be considered high risk AI use by the Act and as the provider the requisite governance is provided alongside our AI system products

The obligations of the Act for Content Guru as the AI system provider and our customers as deployers are completed through contractual and technical controls.

AI Framework in Summary

Content Guru in line with multiple regulations, particularly the EU AI Act 2024 (Regulation (EU) 2024/1689), defined and underpins the (CG) company AI policy set, an operating framework that mirrors the key regulatory principles and needs; focussed on ‘Unacceptable Risk, High Risk, Limited Risk, Minimal Risk’.



Model reference: EU AI Act regulatory framework 2024

- Unacceptable risk: for example, AI systems that allow "social scoring" by governments or companies are considered a clear threat to people's fundamental rights and are therefore banned by the EU AI Act itself.
- High risk: high-risk AI systems such as AI-based medical software or AI systems used for recruitment must comply with strict requirements, including risk-mitigation systems, high-quality of data sets, clear user information, human oversight, etc.
- Specific transparency risk: systems like chatbots must clearly inform users that they are interacting with a machine, while certain AI-generated content must be labelled as such.
- Minimal risk: most AI systems such as spam filters and AI-enabled video games face no obligation under the AI Act, but companies can voluntarily adopt additional codes of conduct.

Content Guru approach in Detail

Content Guru has utilised information from multiple sources and adheres to the EU framework as noted in the summary above and detailed below.

Unacceptable risk

All AI systems considered a clear threat to the safety, livelihoods and rights of people are banned. The EU **AI Act prohibits eight practices**:

1. Harmful AI-based manipulation and deception
2. Harmful AI-based exploitation of vulnerabilities
3. Social scoring
4. Individual criminal offence risk assessment or prediction
5. Untargeted scraping of the internet or CCTV material to create or expand facial recognition databases
6. Emotion recognition in workplaces and education institutions
7. Biometric categorisation to deduce certain protected characteristics
8. Real-time remote biometric identification for law enforcement purposes in publicly accessible spaces

High risk

AI use cases that can pose serious risks to health, safety or fundamental rights are classified as high-risk and include:

- AI safety components in critical infrastructures (e.g., transport), the failure of which could put the life and health of citizens at risk
- AI solutions used in education institutions, that may determine the access to education and course of someone's professional life (e.g., scoring of exams)
- AI-based safety components of products (e.g., AI application in robot-assisted surgery)
- AI tools for employment, management of workers and access to self-employment (e.g., CV-sorting software for recruitment)
- Certain AI use-cases utilised to give access to essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)
- AI systems used for remote biometric identification, emotion recognition and biometric categorisation (e.g., AI system to retroactively identify a shoplifter)
- AI use-cases in law enforcement that may interfere with people's fundamental rights (e.g., evaluation of the reliability of evidence)
- AI use-cases in migration, asylum and border control management (e.g., automated examination of visa applications)
- AI solutions used in the administration of justice and democratic processes (e.g., AI solutions to prepare court rulings)

High-risk AI systems are subject to strict obligations before they can be put on the market:

- Adequate risk assessment and mitigation systems
- High-quality of the datasets feeding the system to minimise risks of discriminatory outcomes
- Logging of activity to ensure traceability of results
- Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance
- Clear and adequate information to the deployer
- Appropriate human oversight measures
- High level of robustness, cybersecurity and accuracy

Transparency risk

This refers to the risks associated with a need for transparency around the use of AI. The AI Act introduces specific disclosure obligations to ensure that people (defined specifically as humans) are informed when necessary to preserve trust. For instance, when using AI systems such as chatbots, the act defines 'humans', should be made aware that they are interacting with a machine so they can take an informed decision. Any solution designed and delivered by Content Guru will have assured this option is available and in place for customers to implement.

Moreover, providers of generative AI have to ensure that AI-generated content is identifiable. On top of that, certain AI-generated content should be clearly and visibly labelled, namely deep fakes and text published with the purpose to inform the public on matters of public interest. Thus the Content Guru principle framework and our (CG) 'secure/AI design principles' comes into force.

Minimal or no risk

The AI Act does not introduce rules for AI that is deemed minimal or no risk. As organisations like at CG, we must assess and understand if anything we produce meets these criteria. The EU AI Act deems the majority of AI systems currently used fall into this category. For example, this includes applications such as AI-enabled video games or spam filters.

How data is managed

Content Guru manages all media i.e., data, voice recordings etc in line with regulatory, legislation and customer contracted terms. In addition to this, specific Data Privacy regulations (see following section) exist and govern the ways we manage media. Further, for example, in Azure OpenAI abuse monitoring detects and mitigates instances of recurring content and/or behaviours that suggest use of the service in a manner that may violate the code of conduct or other applicable product terms. To detect and mitigate abuse, Azure OpenAI stores all prompts and generated content securely for up to thirty (30) days.

The data store, where prompts and completions are stored, is logically separated by customer resource (each request includes the resource ID of the customer's Azure OpenAI resource). A separate data store is located in each geography in which the Azure OpenAI Service is available, and a customer's prompts and generated content are stored in the Azure geography where the customer's Azure OpenAI service resource is deployed, within the Azure OpenAI service boundary.

No customer data is used for AI learning unless explicitly agreed beforehand.

Where data is processed

Platform	LLM
UK	UK/EU
EU	EU
US	US
JP	JP

Regulation

All Content Guru product data processing managed by AI is also governed by standard contractual Data Processing Agreements in place with our customers and, additionally with business partners that may act as subprocessors. These are underpinned primarily by the UK GDPR and EU GDPR regulation but also meet any necessary regional regulations / legislations.

Compliance with GDPR's Data Protection & EU AI Act by Design and Default

Content Guru ensures **storm** follows GDPR guidelines on data protection by design and default throughout its project lifecycle:

- **Minimization of Data: storm** collects only data strictly necessary for processing and retains it only as long as needed.
- **Pseudonymization and Anonymization:** Where possible, personal data in **storm** is pseudonymized or anonymized to enhance security.
- **Default Privacy Settings: storm** ensures that the most privacy-friendly settings are enabled by default for users.
- **Data Mapping and DPIA:** Comprehensive data mapping is conducted to understand the flow of personal data within **storm**, and Data Protection Impact Assessments (DPIAs) are performed to address privacy risks with customers and third parties.
- **Transparency and Control: storm** provides clear, accessible options for users to understand and control how their data is processed.
- **Rating/Scoring -** Content Guru systems are not designed for, or the use of 'rating' individuals or their emotions, but can/is intended for 'rating' quality of calls, data e.g., abuse language during a call could be rated as 'zero' for professionalism, but cannot in line with the EU AI Act be rated for 'emotion'.

Change control & maintenance

Content Guru employs a robust change control process to ensure that any modifications to **storm** are managed securely and systematically:

- **Change Request and Approval:** All changes to storm go through a formal request and approval process, documented with a clear impact assessment.
- **Risk Assessment:** Each change is evaluated for potential security implications before implementation.
- **Testing in Controlled Environments:** Changes are rigorously tested in isolated test environments to validate functionality and ensure no adverse security impacts on Storm.
- **Audit Trails:** A complete audit trail is maintained, documenting every change request, approval, implementation, and test result.
- **Roll-back Mechanisms:** Contingency plans are in place for rapid roll-back in case a change introduces unforeseen issues.

Content Guru as part of this model, when using third parties such as here, employs a robust contract and change process to ensure that third parties assure they update and maintain environments as defined and agreed in SLAs.

Content Guru manages this through third party self-attestations and declarations to meet contractual commitments. Further, Content Guru undertake, where necessary,) onsite visits or agree audits within contractual obligations.

Data Ownership

Ownership of data at all times remains with Content Guru customers. Any data (for example transcription or summarisation) stored on **storm any** data will be stored as per the agreed retention period and will be transferred/deleted at the end of contract term.

Legal and contractual protections

Legal protection or warranties are provided where appropriate and explicitly detailed in individual contracts.

This AI Charter outlines Content Guru's policies and procedures as a provider of AI products and services. It is intended for information purposes only and does not create any contractual or legal obligations, nor does its inclusion on Content Guru's website incorporate the AI Charter into any customer, partner, or supplier agreement.

Data retention and deletion

Data is retained in line with specific contract agreements and terms; also, for example one of CGs AI partners (Microsoft Azure) retain data for 30 days before deletion in line with their abuse policies.

Data is deleted from **storm** on completion of customer service.

Control Sheet

Title	AI Charter
Author(s)	RJS/JLD/RMM/MRA/SCO
Approved by	RJS/MIB
Date	15/09/25
Version	1.0

Copyright and Disclaimer

Content Guru Ltd., part of the Redwood Technologies Group, reserves the right to make changes to the information in this document at any time without notice. Information published in this document is believed to be reliable. However, Content Guru Ltd. assumes no liabilities for inaccuracies or omissions in this document, or liability arising from the use of such information. Furthermore, Content Guru Ltd. assumes no liability for the infringement of patents or other intellectual property rights owned by third parties which may result from the application of this information.

No part of this document may be reproduced or transmitted in any form or by any means electronic or mechanical, for any purpose, without the written permission of Content Guru Ltd.

Content Guru ®, Content Guru Engagement Made Easy®, iACD®, **brain**®, **storm**® and **storm** CKS® are registered trademarks of Content Guru Ltd.

Engagement Made Easy™, **storm** ACT™, **storm** Admin Portal™, **storm** AHEAD™, **storm** ASK™, **storm** BPO™, **storm** CENTREX™, **storm** CONDUCTOR™, **storm** CONTACT™, **storm** CRM™, **storm** DIAL™, **storm** DROP™, **storm** FAX™, **storm** FLOW™, **storm** INBOUND™, **storm** INTEGRATE™, **storm** LINK™, **storm** LOCK™, **storm** LOSS™, **storm** MASK™, **storm** MATRIX™, **storm** MEDIA™, **storm** NUDGE™, **storm** OUTBOUND™, **storm** PATROL™, **storm** PASS™, **storm** PEP™, **storm** PEW™, **storm** PROTECT™, **storm** REACH™, **storm** RECORDER™, **storm** RESPONSE™, **storm** SHIELD™, **storm** SHOUT™, **storm** SIGN-IN™, **storm** SMS™, **storm** SNAP™, **storm** SOCIAL™, **storm** SPEAK™, **storm** STEER™, **storm** STUDIO™, **storm** SURE™, **storm** TACTIC™, **storm** TRADE™, **storm** TRUST™, **storm** UC™, **storm** VIEW™, **storm** WFM™, and **storm** WHO™ are trademarks of Content Guru Ltd.

DNX®, DTA®, iPath®, LOCK®, RedLink®, RedMatrix®, RedResponse®, Redwood Technologies®, RTComposer®, RTConductor®, RTInstantBilling®, RTMonitor®, RTPerformer®, RTSinfonia®, RTStudio® and the Redwood company logo are registered trademarks of Redwood Technologies Ltd.

Digital Network Xchange™, Intelligent Network Xchange™, INX™, RedAlert™, RedBanner™, RedCentrex™, RedContact™, RedDial™, RedFax™, RedMessage™, RedPBX™, RedRecorder™, RedRouter™ and RedSpeak™ are trademarks of Redwood Technologies Ltd.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

All other trademarks are the property of their respective owners.

Content Guru Ltd., Radius Court, Eastern Road, Bracknell, Berkshire, RG12 2UP, United Kingdom

Registered in England No. 05653869
t: +44 (0)1344 852 350
e: sales@contentguru.com
w: www.contentguru.com