convo

Convo Whitepaper (UK version)

Version 1.3
Last Updated: 22 August 2025

Executive Summary

Convo is a secure and accessible mobile application designed to facilitate **Video Relay Service (VRS)** for the Deaf and hard-of-hearing communities. Built with privacy, usability, and compliance at its core, the platform enables real-time communication through qualified British Sign Language (BSL) interpreters, without requiring integration into client IT systems.

This whitepaper outlines the security, privacy, and operational framework that underpins, including our compliance with UK and international standards such as ISO 27001, GDPR, and Cyber Essentials Plus.

Target Audience

This whitepaper is intended for decision-makers, security officers, technical teams, and organisations interested in understanding the Convo platform's security, privacy, and operational framework.

Overview

Convo leverages Agile development and DevOps best practices to deliver secure, scalable, and reliable communication services. Our infrastructure is cloud-native, streamlined for performance, and hardened against security threats.

Key features:

- **Agile Development**: Continuous integration and delivery with frequent updates and improvements.
- **Regular Security Maintenance**: Our support team consistently applies critical patches.
- **Minimal Attack Surface**: Server operating systems are hardened with only approved, essential software pre-installed.

- **Cloud-First Infrastructure**: We use trusted third-party providers with secure virtualisation environments.

- **Minimal Data Collection**: We collect and securely store only essential personal information—name, email, phone number, and address—on our servers.

Users can download the Convo app from trusted sources like the Apple App Store and Google Play. A stable internet connection is the only requirement to initiate secure, real-time video calls with professional interpreters.

User Experience & Accessibility

Convo is designed with accessibility and user experience at the forefront. The app provides:

- **Simple, intuitive navigation** for users to initiate video calls with ease.

- **Adjustable video quality** for users with varying internet speeds or visual preferences.

- **Real-time support** from qualified BSL interpreters is available on demand without complicated setup or integration.

The app prioritises the needs of Deaf and hard-of-hearing individuals, offering straightforward access to professional interpreters and ensuring the process remains as seamless as possible.

Compliance & Certifications

Convo is committed to maintaining the highest standards in cybersecurity, privacy, and regulatory compliance:

- **ISO 27001**
  Our Information Security Management System (ISMS) ensures a structured approach to managing sensitive information securely.

- **Cyber Essentials Plus**
  Independently verified to protect against the most common cyber threats.

- **UK GDPR & ICO Compliance**
  Full compliance with the UK Data Protection Act and GDPR, under the Information Commissioner's Office (ICO) guidance.

- **Data Protection Impact Assessment (DPIA)**:
  To ensure GDPR compliance and protect user privacy, we conduct **DPIA** whenever new data processing activities are introduced. The DPIA evaluates potential risks to privacy and ensures these are mitigated through appropriate technical and organisational measures. It also assesses the necessity and proportionality of data processing to address any risks before new projects or changes are implemented.

- **PCI DSS v4.0 (Level 1)**
  Ensures secure handling of payment data in line with the highest industry standards.

- **Penetration Testing**
  Annual third-party penetration tests, with additional testing conducted after significant platform updates.

- **Vulnerability Scanning**
  Conducted 3–4 times monthly using commercial-grade tools to identify and remediate risks proactively.

Data Security & Privacy

Convo adopts a comprehensive approach to data protection, ensuring all personal and communication data is handled lawfully, securely, and transparently.

1. Data Collection & Minimisation

We collect only the minimum data required for account creation and support:

- Full name
- Date of Birth
- Email address
- Phone number
- Address (for billing or account management

We do **not** collect or retain unnecessary personal data or call content.

2. Data Processing & GDPR Compliance

- We act as a **Data Controller** under GDPR, processing data only for legitimate business purposes.
- All processing activities are transparent, with user rights clearly defined (access, correction, deletion).
- Data handling follows principles of lawfulness, fairness, purpose limitation, and data minimisation.

3. Encryption & Secure Transmission

- **At Rest**: AES-256-GCM encryption is used for all stored personal data.
- **In Transit**: TLS 1.2 and SSH are used to secure data transmissions.
- Passwords are hashed with **BCryptPasswordEncoder**, and credential tokens are securely encrypted.

4. Video Relay Call Handling

- No video, audio, or transcript data is stored after a call.
- Interpreters receive only live communication data, which is not retained.
- Sessions are fully encrypted, with strict access limited to verified, qualified interpreters.

5. Backups & Geo-Redundancy

- Secure, encrypted backups are performed continuously.
- We use ISO 27001-certified cloud vendors across multiple regions for geo-redundancy.

Network Security

Our cloud systems are secured with a firewall that limits IP addresses and port numbers, enabling secure and smooth communication between clients and cloud providers. We employ multiple layers of network defence to ensure system integrity and continuity:

- **Firewalls & IP Filtering**: Restrict access by port, protocol, and origin.
- **Access Controls**: Implemented through Network Access Control Lists (NACLs) and Security Groups.**TLS 1.2 encryption** ensures data is secure across all network layers.
- Flow chart: The network chart can be provided upon request.
- Data is routed through **DNS management, traffic monitoring, Network Access Control Lists (NACLs), and Security Groups**.

Application Security

Security is integrated throughout the software development lifecycle:

- **Code Review & Testing**: All development undergoes peer review and automated testing.
- **Secure Coding Standards**: Developers follow OWASP and NIST 800-53
- **Automated Security Scans**: Tools like AWS Inspector, OpenVAS, Nessus, and BurpSuite Pro are used regularly.
- **Vulnerability Remediation**: Patching and mitigation follow strict SLAS.

Business Security

Convo has robust internal and vendor-focused security processes in place:

convo

1. Vendor Management

- All third-party vendors undergo security and compliance due diligence.
- Critical vendors are reviewed annually with financial, legal, and operational risk assessments.

2. Security Governance

- Convo follows National Institute of Standards and Technology and ISO 27001-aligned security frameworks.
- A contracted security partner oversees penetration testing, incident response, and ongoing risk management.

3. Employee Security

- **Background Checks**: Conducted only for roles where deemed necessary and relevant.
- **Confidentiality Agreements**: All staff and contractors sign confidentiality agreements.
- **Security Training**: Mandatory cybersecurity training at hiring and annually, covering phishing, data handling, and incident response.

Breach Notification Process

In the event of a personal data breach, Convo is committed to prompt action and full GDPR compliance:

- **Immediate Response**: Upon breach identification, we will act swiftly to contain and assess the situation to minimise further risks.

- **Notification to Affected Users**: Affected users will be informed within 72 hours via their registered email addresses, as required by **GDPR Article 33**. The notification will include:

    - A description of the breach and data involved.
    - The likely consequences.
    - Steps taken to address the breach.

- **Notifying Supervisory Authorities**: If the breach poses a high risk, we will notify the relevant supervisory authority within 72 hours.

- **Ongoing Communication**: We will provide further updates to affected individuals as necessary and offer guidance on protective measures.

- **Post-Breach Review**: A thorough investigation will identify the root cause and implement corrective actions to prevent future breaches.

convo

Physical & Cloud Infrastructure Security

Convo does not operate physical servers. Instead, we partner with **ISO 27001-certified cloud providers** to host our infrastructure securely and regionally:

- **UK Region** – London (AWS)
- **Australia** – Sydney (ap-southeast-2)
- **USA** – N. Virginia (us-east-1)

Cloud provider security includes:

- Physical access restrictions
- Biometric authentication
- 24/7 monitoring and surveillance
- Environmental controls and redundancy systems

Conclusion

Convo is dedicated to providing secure, accessible, and privacy-first video communication services. Our commitment to international standards, continuous security enhancements, and focus on user trust ensures that every Video Relay Service (VRS) call remains protected, private, and seamless.

By eliminating the need for client-side integration, Convo empowers organisations and individuals to engage in confidently interpreted conversations in real-time, anytime, anywhere. We uphold the highest security standards by implementing rigorous security controls, adhering to regulatory requirements, and continuously enhancing our security measures to safeguard customer data.

The Convo app does not require integration with any client IT system or access to client data. Users can easily download the app from trusted platforms like the Apple App Store and Google Play. A stable internet connection is needed to initiate secure Video Relay Service (VRS) calls. Designed to be user-friendly and accessible, Convo ensures a smooth experience while maintaining robust data security and privacy.

Once downloaded, users can connect with others via video communication, regardless of their location or device, as long as they have reliable internet access. Trusted app stores with strong security measures assure users of the app's authenticity and safety.