WHITEPAPER

GDPR and the CLOUD Act Risk in Video Communications

Why organisations in regulated sectors can no longer treat platform jurisdiction as a footnote

Author
Andy Esser, CTO
haia.live

Published
March 2025

Classification
Public | Version 1.2

EXECUTIVE SUMMARY

Organisations in defence, healthcare, and financial services routinely transmit sensitive, regulated, and sometimes classified information through video communication platforms headquartered in the United States. Most are unaware that doing so creates a structural legal conflict between the EU GDPR and the US CLOUD Act.

This conflict cannot be resolved by contractual safeguards, data processing agreements, or the existence of European data centres operated by US companies. This paper sets out the nature of that conflict, its practical implications for regulated sectors, and the architecture characteristics of a communications platform that eliminates the exposure at source.

haia.live is registered in the United Kingdom and operates on EU infrastructure in Frankfurt, Germany. This paper addresses directly whether UK registration combined with EU data processing satisfies the legal requirements of regulated organisations, including those with EU-facing obligations.

1. The Regulatory Landscape

1.1 GDPR in Brief

The General Data Protection Regulation (EU 2016/679) came into full effect in May 2018 and remains the most significant data protection framework in the world. For organisations handling personal data in connection with EU residents, regardless of where the organisation itself is headquartered, GDPR imposes obligations around lawfulness of processing, data minimisation, purpose limitation, and restrictions on the transfer of personal data to third countries.

Chapter V of GDPR (Articles 44 to 50) prohibits transfers of personal data to countries outside the European Economic Area unless one of a limited set of conditions is met: an adequacy decision by the European Commission, appropriate safeguards such as Standard Contractual Clauses, or explicit consent from the data subject in limited circumstances. The underlying principle is that the level of protection afforded to individuals must not be undermined by cross-border data flows.

1.2 The US CLOUD Act

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act), enacted by the United States Congress in March 2018, grants US law enforcement agencies the authority to compel US-based technology companies to produce data stored anywhere in the world, including on servers physically located within the European Union, without requiring notification of the data subject or the relevant EU authority.

Critically, the CLOUD Act applies to any company subject to US jurisdiction: any company incorporated in the United States, with its principal place of business in the United States, or organised under US law. It is not a question of where data is stored. A US company operating a data centre in Frankfurt remains subject to CLOUD Act compulsion for data processed on that infrastructure.

KEY LEGAL TENSION

GDPR Article 48 states explicitly that any judgment, decision, or order of a court or tribunal in a third country which requires a controller or processor to transfer or disclose personal data may only be recognised or enforceable if based on an international agreement in force between the requesting third country and the EU.

No such comprehensive agreement exists between the US and the EU that would subordinate CLOUD Act requests to GDPR. The two laws are in direct structural conflict.

1.3 The Collapse of Privacy Shield and Its Aftermath

The legal uncertainty surrounding US-EU data transfers is not theoretical. In July 2020, the Court of Justice of the European Union invalidated the EU-US Privacy Shield framework in the Schrems II decision, ruling that US surveillance laws did not offer EU residents an equivalent level of protection to that guaranteed by GDPR.

The EU-US Data Privacy Framework, adopted in July 2023, provides a replacement adequacy mechanism. However, it has already been challenged before the CJEU by privacy advocates and legal observers consider it vulnerable to the same structural objections that felled Privacy Shield, namely that US law authorises forms of surveillance access that GDPR does not permit. Organisations relying on the Data Privacy Framework as their sole transfer mechanism are accepting a regulatory risk that may materialise without warning.

2. The haia.live Jurisdictional Position

2.1 UK Incorporation, EU Infrastructure

haia.live is registered and headquartered in the United Kingdom, and operates its data processing infrastructure from EU-based data centres in Frankfurt, Germany. This combination requires careful legal analysis, because it involves two separate questions: what law governs the company, and where is the data physically processed.

The answer to the first question is straightforward and highly favourable. haia.live is a UK company, subject to UK law, and wholly outside the reach of US legal compulsion. A US court cannot issue a CLOUD Act order to haia.live. There is no US parent company, no US beneficial ownership, and no operational dependency on US-incorporated entities. This is the structural immunity that US-headquartered platforms cannot offer regardless of where they locate their servers.

The answer to the second question is also favourable. Frankfurt is within the European Union. Data processed on haia.live infrastructure is processed on servers located in an EU member state, under German and EU law. German data protection law and the enforcement jurisdiction of the relevant German data protection authorities apply to the processing activities that take place there.

2.2 The Transfer Question: EEA Organisations Sending Data to haia.live

For EU and EEA-based organisations, transmitting personal data to haia.live for processing involves a transfer from the EEA to the UK under the EU GDPR, because haia.live as a company is UK-incorporated. This transfer requires a lawful transfer mechanism.

That mechanism exists and is currently robust. The European Commission renewed its adequacy decision for the UK in December 2025, valid until December 2031. This decision confirms that the UK's data protection framework, the UK GDPR as enforced by the Information Commissioner's Office, provides a level of protection essentially equivalent to that of the EU GDPR. EEA organisations can therefore transfer personal data to haia.live without Standard Contractual Clauses or any other supplementary safeguard.

Importantly, once that data reaches haia.live's processing infrastructure in Frankfurt, it is being processed within the EU. It does not leave EU territory. The data flow is: EEA organisation to UK company (covered by adequacy) with actual processing occurring on EU soil.

THE haia.live LEGAL POSITION IN SUMMARY

UK company: outside US CLOUD Act jurisdiction entirely. No US court can compel disclosure.

EU infrastructure (Frankfurt): all data processing occurs within the European Union. Data does not leave EU territory during processing.

UK adequacy decision: transfers from EEA organisations to haia.live are lawful without SCCs, under the EU Commission adequacy decision for the UK, renewed December 2025 and valid until December 2031.

UK GDPR compliance: haia.live is subject to the UK GDPR, enforced by the ICO, which the EU Commission has assessed as providing equivalent protection to the EU GDPR regime.

Result: EEA customers can use haia.live with a clear legal basis for data transfer, full GDPR-equivalent protection, and none of the CLOUD Act exposure that applies to every major US-

headquartered competitor.

2.3 Honest Caveats

Intellectual honesty requires acknowledging areas that data protection professionals and procurement teams should understand when assessing haia.live against a purely EU-incorporated alternative.

The adequacy decision is subject to review

Unlike EU membership, UK adequacy status is subject to periodic review and can in principle be withdrawn if the EU Commission determines that the UK's data protection framework has diverged from EU standards. The current decision runs until December 2031 and carries a monitoring obligation throughout. The European Data Protection Board has confirmed its general satisfaction with UK-EU alignment, and the practical and diplomatic costs of withdrawal are high. Organisations making long-term platform commitments should be aware of this dynamic, though the current legal position is clear.

National security exemptions are under monitoring

The EDPB's opinion on the 2025 renewal noted specific concerns about national security exemptions in UK law, including provisions in the Investigatory Powers Amendment Act 2024 that allow certain data protection principles to be disapplied in national security contexts. For commercial data processing, including enterprise video communications, these exemptions are not directly applicable. Defence sector organisations should note that the UK's national security access powers are subject to ongoing Commission monitoring as a condition of continued adequacy.

The UK GDPR will continue to evolve independently

The UK government has powers under the Data (Use and Access) Act 2025 to modify the data protection framework by secondary legislation, including in areas such as international transfers and automated decision-making. While the EDPB has confirmed that the current framework remains essentially equivalent to the EU GDPR, divergence remains a future possibility. Organisations should keep this under review, particularly for multi-year contracts.

2.4 Comparison with US Platform Exposure

The relevant comparison for most organisations is not between haia.live and a hypothetical EU-incorporated alternative. It is between haia.live and the US-headquartered platforms that currently dominate the market. On that comparison, the position is clear.

Dimension	haia.live vs US platforms (Teams, Zoom, Google Meet, Webex)
CLOUD Act exposure	None for haia.live. UK company, not subject to US law. All four major US platforms are subject to CLOUD Act compulsion regardless of where data is stored.
Data processing location	EU infrastructure (Frankfurt). Data stays within the EU. US platforms route data through US infrastructure by default.
Lawful basis for EEA transfers	UK adequacy decision in force until December 2031. No additional safeguards required. US platforms require the Data Privacy Framework, which is under active CJEU challenge.
Secret disclosure risk	Not present. haia.live cannot receive a gag-order CLOUD Act

	demand from a US court. US platforms have been served with classified CLOUD Act orders.
Supervisory authority	UK ICO, assessed by EU Commission as providing equivalent protection. US platforms are subject to US regulatory oversight only.
Governing data law	UK GDPR, functionally equivalent to EU GDPR for current purposes. US platforms are governed by US law at the company level.

3. Video Communications: A Particular Exposure

3.1 What Is Transmitted in a Video Call

Video conferencing is frequently treated as a casual, ephemeral communication channel. In practice, modern video platforms transmit and process a significantly broader range of data:

- Audio and video streams, including metadata about participants
- Chat messages, shared files, and screen-share content
- Meeting recordings, transcripts, and AI-generated summaries
- Participant identifiers, IP addresses, and device information
- Calendar integration data, contact lists, and scheduling information
- Usage analytics, including attendance, duration, and engagement patterns

In regulated sectors, the content of these communications routinely includes patient clinical information, financial transaction details, legal advice, procurement specifications, or information that is operationally sensitive in a defence context. The platform carrying these communications sits at the centre of a significant data protection obligation.

3.2 The Market Dominance of US Platforms

The global video communications market is dominated by a small number of US-headquartered providers: Microsoft (Teams), Zoom, Google (Meet), and Cisco (Webex). All four are incorporated under US law and therefore subject to CLOUD Act compulsion. All four have significant European customer bases in regulated sectors.

Platform	US jurisdiction and CLOUD Act exposure
Microsoft Teams	Microsoft Corporation, incorporated in Delaware. Subject to CLOUD Act. European data centre option does not remove US legal exposure.
Zoom	Zoom Video Communications Inc, incorporated in Delaware. Subject to CLOUD Act. Data routed through US infrastructure by default.
Google Meet	Alphabet Inc, incorporated in Delaware. Subject to CLOUD Act. Part of Google Workspace, processed under US terms.
Cisco Webex	Cisco Systems Inc, incorporated in California. Subject to CLOUD Act. Same jurisdictional exposure applies.

3.3 The European Data Centre Misconception

One of the most persistent misunderstandings in this area is the belief that a US company operating data centres within the EU resolves the jurisdictional problem. It does not. The CLOUD Act applies to the company, not to the infrastructure. A US court can compel Microsoft, Zoom, or Google to produce data held on servers in Frankfurt, Dublin, or Amsterdam in precisely the same way it can compel production of data held in Virginia.

This is the critical distinction between haia.live and those platforms. When haia.live operates infrastructure in Frankfurt, the data is processed by a UK company that is not subject to US law.

When Microsoft operates infrastructure in Frankfurt, the data is processed by a US company that is subject to US law. The physical location is the same. The legal exposure is entirely different.

PRACTICAL ILLUSTRATION

A hospital trust uses Microsoft Teams for clinical consultations. Patient data, including audio, video, and clinical notes shared in chat, is processed by Microsoft Corporation, a US entity.

A US authority issues a CLOUD Act order requiring Microsoft to produce communications relating to a particular individual. Microsoft is legally required to comply. The hospital trust is not notified. The transfer occurs without a legal basis under GDPR. The hospital trust is exposed to a breach it cannot detect, prevent, or remediate.

The same hospital trust using haia.live faces no equivalent risk. haia.live is a UK company. A US court has no jurisdiction over it. No CLOUD Act order can be served.

4. Sector-Specific Risk Analysis

4.1 Defence and National Security

For organisations operating in the defence sector, including government departments, defence contractors, armed forces, and intelligence-adjacent agencies, the risk profile of US-platform video communications extends beyond data protection law. Information discussed in operational or procurement contexts may be subject to classification requirements, official secrets legislation, or defence export controls.

CLOUD Act requests can compel disclosure without notification to the subject organisation and without any opportunity to invoke privilege or classification. A defence contractor discussing procurement specifications over a US-platform video call has no mechanism to prevent that content from being disclosed to a US authority, even if the communication would otherwise be subject to legal privilege or security classification under UK or EU law.

NATO members are increasingly sensitised to this exposure. The UK's National Cyber Security Centre and Germany's Federal Office for Information Security (BSI) have both published guidance addressing the risks of third-country data access in communications tools. Several allied governments have issued policies restricting the use of US-headquartered platforms for certain categories of sensitive discussion.

4.2 Healthcare

Healthcare organisations are subject to a particularly dense regulatory environment. GDPR categorises health data as special category data under Article 9, attracting a higher standard of protection. In the UK, the NHS Data Security and Protection Toolkit and the common law duty of confidentiality impose additional obligations. In EU member states, sector-specific health data legislation adds further requirements.

Clinical video consultations, which proliferated during the COVID-19 pandemic and have become a permanent feature of care delivery, involve the transmission of health data, conversation about diagnoses and treatment plans, and often the display or discussion of medical records. The use of US-platform tools for these consultations creates a structural conflict with GDPR Article 9 and the obligation of professional confidentiality that clinicians carry.

- NHS organisations must demonstrate DSPT compliance, which includes requirements around information governance and third-party data processing
- GDPR requires explicit, granular consent or another Article 9 basis for processing health data, which cannot be obtained through generic platform terms of service
- AI transcription and meeting summary features offered by US platforms may involve processing health data for purposes beyond the original clinical intent
- Patients have a reasonable expectation that clinical conversations are confidential; a US government data access request would breach that expectation without their knowledge

4.3 Financial Services

Financial services organisations face specific obligations around data governance, third-party risk management, and operational resilience. In the EU, the Digital Operational Resilience Act (DORA), which entered full enforcement in January 2025, requires financial entities to conduct detailed assessments of ICT third-party risks, including the legal and jurisdictional risks associated with technology providers headquartered outside the EU.

MiFID II record-keeping requirements mandate that certain communications, including those relating to transactions and client advice, are recorded and retained with guaranteed integrity and

accessibility. If those recordings are stored on infrastructure subject to CLOUD Act compulsion, the confidentiality of regulatory records is potentially compromised without the financial entity's knowledge.

The European Banking Authority and the European Insurance and Occupational Pensions Authority have published guidelines on outsourcing arrangements that include requirements to assess the legal risks associated with the laws of the country where a service provider is headquartered, which is directly relevant to the choice of video communications platform.

5. The Limits of Standard Contractual Clauses

Standard Contractual Clauses are the most widely used mechanism for GDPR-compliant data transfers to third countries. They are contract terms approved by the European Commission that data exporters and importers use to provide appropriate safeguards for personal data. Following the Schrems II ruling, the Commission issued revised SCCs in June 2021 that include a requirement for data importers to notify the exporter if they receive a request for disclosure from a public authority.

However, SCCs are a contractual mechanism; they bind the parties to the contract, but they cannot override US law. If a US company subject to CLOUD Act compulsion is ordered by a US court to produce data, its SCC obligations are subordinate to that court order. The company may be legally required to produce the data without being permitted to notify the European exporter, because the CLOUD Act includes provisions allowing courts to impose gag orders on recipients of data demands.

LEGAL REALITY

SCCs provide a useful legal framework for routine cross-border data transfers and demonstrate a good faith effort at GDPR compliance. They do not provide protection against covert data access under US surveillance law, because they do not bind US courts or US law enforcement agencies.

A data processor that receives a classified CLOUD Act demand may be prohibited from disclosing its existence to the data controller, meaning the controller cannot fulfil its own GDPR obligations to data subjects. No contract between private parties can resolve this structural gap.

For transfers to haia.live from EEA organisations, SCCs are not required and this problem does not arise. The UK adequacy decision provides a clean, straightforward legal basis for the transfer.

The revised SCCs require data importers to conduct a Transfer Impact Assessment: an analysis of whether the laws of the importer's country allow authorities to access personal data in a way that goes beyond what is necessary and proportionate. Every honest assessment conducted in respect of a US-headquartered provider must acknowledge the CLOUD Act as a mechanism for non-notified, judicially compelled data access. Many organisations are conducting these assessments but treating them as a compliance formality rather than a genuine risk evaluation.

6. AI Features: An Additional Exposure Vector

The rapid integration of AI-powered features into video communication platforms has introduced an additional dimension to the jurisdictional risk. Major US platforms now offer AI-generated meeting transcription, real-time translation, action item extraction, meeting summaries, and coaching tools based on communication patterns. These features involve processing the raw content of communications, including audio, video, and text, by AI systems that may be operated by the platform provider or by third parties.

For regulated sectors, this creates several specific concerns:

- Training data: AI models may be trained on communication data. Even where providers claim not to train on customer data by default, contractual terms have changed repeatedly and consent mechanisms are frequently opaque.
- Sub-processor exposure: AI feature providers may be additional sub-processors not clearly disclosed in the main privacy documentation, each introducing their own jurisdictional profile.
- Purpose limitation: GDPR requires that personal data is processed only for specified, explicit, and legitimate purposes. Using patient or client communication data to improve AI models may not be compatible with the original collection purpose.
- Data retention: AI-generated summaries and transcripts may be retained for longer than the original recording, held in systems operated by the AI provider rather than the platform provider.

A video communications platform designed for regulated sectors should be unambiguous on these points: no AI processing of call content, no third-party AI sub-processors with access to communication data, and no training of models on customer communications under any circumstances.

haia.live does not use AI to process, analyse, or learn from call content. There are no AI-generated summaries, transcription services, or coaching features that touch the substance of communications. This is an architectural principle, not a configurable setting.

7. What a Compliant Platform Looks Like

The characteristics of a video communications platform that addresses the structural legal risks described in this paper are primarily jurisdictional and architectural. Technology can deliver security; jurisdiction determines whether that security can be legally undermined.

7.1 Jurisdiction Outside US Reach

The fundamental requirement is that the platform provider is incorporated and headquartered in a country not subject to US legal compulsion and without analogous domestic legislation enabling covert government access to commercial data. UK registration satisfies this requirement. haia.live is a UK-incorporated company with no US parent, no US beneficial ownership, and no operational dependency on US-incorporated entities.

7.2 Data Processing Within the EU

haia.live processes all customer data on infrastructure located in Frankfurt, Germany. All call content, metadata, recordings, and associated administrative data remains within the European Union throughout processing. This means that the substantive protections of EU law, including the GDPR and the enforcement jurisdiction of German data protection authorities, apply directly to the data at rest and in transit.

This is distinct from the position of US platforms offering European data centres: those platforms keep data on EU soil but under the governance of a US company subject to US law. haia.live keeps data on EU soil under the governance of a non-US company not subject to US law.

7.3 The Transfer Chain for EEA Customers

EEA organisations sending data to haia.live rely on the UK adequacy decision as their transfer mechanism. This is a full adequacy finding, renewed in December 2025, valid until December 2031, requiring no supplementary contractual safeguards. Organisations should document this in their records of processing activities. For added prudence, haia.live can also support a Data Processing Agreement incorporating the UK Addendum to the EU SCCs as a contingency mechanism.

7.4 End-to-End Encryption and Key Control

End-to-end encryption, with keys held by the customer rather than by haia.live or any third party, provides a technical layer of protection that complements the jurisdictional architecture. Even in the unlikely event of a lawful UK access request, encrypted content to which haia.live does not hold the keys cannot be meaningfully disclosed.

7.5 Regulatory Alignment

Requirement	haia.live characteristic
EU GDPR Chapter V: lawful EEA-to-UK transfers	UK adequacy decision in force until December 2031. No SCCs required.
GDPR Article 9: special category data	End-to-end encryption. No AI processing of content. Full DPA available.
GDPR Article 28: processor obligations	UK-based controller/processor. Full sub-processor transparency. Customer key option.
Data processing location	Frankfurt, Germany. All data remains within the EU throughout processing.

CLOUD Act immunity	UK company, not subject to US law. US courts have no jurisdiction.
DORA ICT third-party risk	UK-domiciled provider. Documented resilience. Contractual audit rights available.
NHS DSPT / UK IG requirements	UK data controller. EU infrastructure. No third-country transfers. Clinically confidential by architecture.
NIS2 (EU critical infrastructure)	EU infrastructure. Security-by-design. Incident reporting compatible.
No AI training on communications	Architectural principle. Call content is never processed by AI systems.

8. Practical Recommendations

Organisations in regulated sectors should take the following steps to assess and address their video communications exposure.

Conduct an honest Transfer Impact Assessment

If your organisation uses US-headquartered video communication platforms, conduct a genuine Transfer Impact Assessment. Document the CLOUD Act exposure, the absence of a comprehensive mutual legal assistance treaty that would subject US data demands to GDPR, and the limitations of SCCs as a mitigating measure. Retain this assessment for regulatory inspection.

Map your communication content to data categories

Catalogue what information is routinely transmitted through your video communications infrastructure. Where this includes special category data, legally privileged information, classified material, or data subject to sector-specific confidentiality obligations, the risk profile of US-platform usage is materially elevated.

Review AI feature terms carefully

For any platform where AI features are enabled, including transcription, summaries, and coaching tools, review the current terms of service. Identify which sub-processors have access to communication content, where AI processing occurs, and what data retention periods apply. Disable features that cannot be brought into compliance with your legal obligations.

Assess procurement framework coverage

In healthcare and public sector contexts, check whether your current platform is procured through a framework agreement and whether the framework assessment adequately addresses third-country jurisdiction risks. Framework listing is not a GDPR compliance guarantee.

Evaluate UK and European alternatives with rigour

When assessing UK or European-headquartered alternatives, apply the same rigour you would to any high-risk vendor. Verify: country of incorporation and ultimate beneficial ownership; data processing infrastructure location and jurisdiction; sub-processor list; encryption architecture and key management; AI policy; and regulatory certifications. Certification alone does not address jurisdictional exposure.

Document your decision and the rationale

Whether you continue with a US-headquartered platform or transition to a UK or European alternative, document your risk assessment and the rationale for your decision. Regulators will want to see evidence of considered decision-making, not just the outcome.

9. Conclusion

The conflict between GDPR and the US CLOUD Act in the context of video communications is a structural exposure that exists whenever a regulated organisation uses a US-headquartered platform to conduct communications involving personal data. That covers virtually every professional video call.

The exposure cannot be resolved by contractual mechanisms, data residency claims, or Standard Contractual Clauses, because none of these instruments bind US courts or US law enforcement agencies. The only structural solution is to use a platform that falls outside US jurisdiction entirely.

haia.live satisfies this requirement. It is incorporated in the United Kingdom, subject to UK GDPR and ICO oversight, with no US parent company and no exposure to US legal compulsion. Its processing infrastructure is located in Frankfurt, Germany, within the European Union, meaning that all data remains on EU soil throughout its lifecycle. Transfers from EEA organisations are lawful under the EU adequacy decision for the UK, renewed in December 2025 and valid until December 2031.

The UK adequacy decision is not a permanent guarantee, and organisations with multi-year commitments should keep the position under review. It is, however, the most legally straightforward transfer mechanism currently available for UK-based processors and is not subject to the same structural vulnerabilities as the Data Privacy Framework, which governs transfers to US entities and remains under active legal challenge.

For organisations in defence, healthcare, and financial services, the question is whether the fundamental confidentiality obligations they carry, to patients, to clients, to counterparties, and to the state, can be honoured when their communications infrastructure is legally accessible to a foreign government without notification or recourse.

haia.live was built on the premise that for regulated organisations the answer to that question should be clear.

About haia.live

haia.live is a UK-registered video communications platform built for organisations that cannot afford to treat data sovereignty as an afterthought. haia.live processes all communication data on EU infrastructure in Frankfurt with no US-jurisdiction exposure, no AI training on call content, and no dependency on US parent companies. haia.live is designed for the regulatory requirements of healthcare, financial services, legal, and public sector organisations.