Transfer Impact Assessment

qualcode.ai

Assessment of US Data Transfers for AI Sub-processors

Version: 1.0
Assessment Date: January 2026
Next Review: January 2027

AI Research & Technology Lab GmbH
Enzersdorfer Strasse 25
A-2340 Modling, Austria

1 Introduction

This Transfer Impact Assessment (TIA) evaluates the risks associated with transferring personal data from the European Economic Area (EEA) to the United States in connection with the qualcode.ai service.

1.1 Purpose

Following the Court of Justice of the European Union's judgment in *Schrems II* (Case C-311/18), organizations transferring personal data to third countries must assess whether the legal framework of the destination country provides essentially equivalent protection to that guaranteed within the EU under the GDPR.

This assessment specifically evaluates our transfers to:

- **OpenAI, Inc.** - AI classification provider (Rater A)
- **Anthropic, PBC** - AI classification provider (Rater B)

1.2 Scope

This TIA covers the transfer of survey response data submitted by our customers (data controllers) for AI-assisted classification. This data may contain personal information about survey respondents.

1.3 Methodology

This assessment follows the European Data Protection Board's recommendations on supplementary measures (Recommendations 01/2020, version 2.0, adopted 18 June 2021) and considers:

1. The nature and volume of data transferred
2. The legal framework of the destination country
3. Contractual safeguards in place
4. Technical and organizational measures
5. Practical likelihood of access by public authorities

2 Transfer Details

2.1 Data Categories Transferred

Category	Description
Survey Responses	Free-text answers to open-ended survey questions, which may contain personal information such as names, opinions, or experiences
Classification Context	Coding guide categories and training examples provided by the customer to guide classification
Metadata	Request identifiers for processing correlation; no personally identifying information

2.2 Volume and Frequency

- **Volume**: Variable depending on customer usage; typically hundreds to thousands of survey responses per coding run
- **Frequency**: On-demand, triggered by customer-initiated coding runs
- **Duration of exposure**: Transient (seconds to minutes for API processing)

2.3 Recipients

Recipient	Purpose	Location
OpenAI, Inc.	AI text classification (GPT-4 series)	USA
Anthropic, PBC	AI text classification (Claude models)	USA

3 US Legal Framework Assessment

3.1 Relevant US Laws

The following US surveillance laws are relevant to this assessment:

3.1.1 FISA Section 702

The Foreign Intelligence Surveillance Act Section 702 authorizes the collection of foreign intelligence information from non-US persons located outside the US through compelled assistance from US electronic communication service providers.

Applicability: OpenAI and Anthropic could potentially be compelled to provide data under FISA 702 if:
- The data relates to “foreign intelligence information”
- The target is a non-US person located outside the US
- A FISA 702 directive is issued by the Foreign Intelligence Surveillance Court

3.1.2 Executive Order 12333

EO 12333 authorizes intelligence collection activities conducted outside the US, including collection of data in transit.

Applicability: Data transmitted to US-based servers transits international networks and could theoretically be subject to EO 12333 collection. However, our use of TLS encryption provides meaningful protection against bulk collection.

3.1.3 CLOUD Act

The CLOUD Act allows US authorities to compel US companies to disclose data stored abroad.

Applicability: Limited relevance as our primary data storage is in the EU, and the AI providers receive only transient API calls, not stored data.

3.2 Post-Schrems II Developments

Since the Schrems II decision, several developments have affected the US legal landscape:

3.2.1 Executive Order 14086 (October 2022)

President Biden signed EO 14086 implementing new safeguards for US signals intelligence activities, including:

- Limiting bulk collection of signals intelligence
- Requiring proportionality and necessity assessments
- Establishing a Data Protection Review Court for EU individuals

3.2.2 EU-US Data Privacy Framework (July 2023)

The European Commission adopted an adequacy decision for the EU-US Data Privacy Framework, finding that the US provides adequate protection for personal data transferred to certified organizations.

Note: As of this assessment date, neither OpenAI nor Anthropic are certified under the DPF. Therefore, we rely on Standard Contractual Clauses (SCCs) as our transfer mechanism.

4 Sub-processor Analysis

4.1 OpenAI, Inc.

4.1.1 Contractual Safeguards

- **Data Processing Addendum**: OpenAI's DPA incorporates the EU SCCs (Commission Decision 2021/914)
- **Limited Data Retention**: Data not used for training; may be retained up to 30 days for abuse detection per API terms
- **No Training**: Data is not used to train or improve OpenAI models
- **Subprocessor List**: OpenAI publishes and updates its subprocessor list

4.1.2 Technical Safeguards

- TLS encryption for all API communications
- Transient processing with no persistence
- Request isolation (no cross-customer data exposure)
- Geographic routing options (though US processing is standard)

4.1.3 Organizational Safeguards

- SOC 2 Type II certification
- Regular security assessments
- Employee training and access controls

4.1.4 Risk Assessment for OpenAI

Factor	Assessment	Rationale
Likelihood of government access	Low	Transient processing, no stored data to compel; survey coding is unlikely to constitute "foreign intelligence information"

Impact if access occurred	Variable	Depends on survey content; most survey responses do not contain sensitive personal data
Effectiveness of safeguards	High	SCCs, encryption, and transient processing provide multiple layers of protection

4.2 Anthropic, PBC

4.2.1 Contractual Safeguards

- **Data Processing Addendum**: Anthropic's DPA incorporates the EU SCCs (Commission Decision 2021/914)
- **Limited Retention Policy**: Data not used for training; may be retained up to 30 days for abuse detection per API terms
- **No Training**: Customer data is excluded from model training
- **Transparency**: Subprocessor list available

4.2.2 Technical Safeguards

- TLS encryption for all API communications
- Ephemeral processing architecture
- Request isolation and access controls
- System-level security monitoring

4.2.3 Organizational Safeguards

- SOC 2 Type II certification
- Security-first organizational culture
- Constitutional AI safety framework

4.2.4 Risk Assessment for Anthropic

Factor	Assessment	Rationale
Likelihood of government access	Low	Transient processing architecture; survey classification unlikely to trigger intelligence interest
Impact if access occurred	Variable	Depends on specific survey content uploaded by customers
Effectiveness of safeguards	High	SCCs, encryption, ephemeral processing, and no data persistence

5 Risk Assessment

5.1 Likelihood of Government Access

We assess the likelihood of US government access to qualcode.ai customer data as **Low to Medium** based on:

1. **Transient processing**: Data is processed in real-time and not used for training. Note: FISA Section 702 applies to communications in transit, not just stored data. AI providers may retain request logs for abuse detection (up to 30 days).
2. **Nature of data**: Survey responses for market research and academic studies are unlikely to constitute "foreign intelligence information" under FISA or to be targets of intelligence collection.
3. **Volume and selectivity**: Any FISA 702 directive would need to be targeted at specific foreign intelligence targets, not bulk academic survey data.
4. **Practical considerations**: US intelligence agencies have finite resources focused on national security priorities. Coded survey responses represent minimal intelligence value.

5.2 Impact Assessment

The impact of potential government access varies based on the nature of data uploaded by customers:

Data Type	Impact	Notes
Standard market research	Low	Brand preferences, product feedback generally not sensitive
Academic opinion surveys	Low-Medium	May include political views; unlikely intelligence target
Surveys with identifiable data	Medium	Names or contact details increase impact if exposed
Sensitive topic surveys	Medium-High	Health, political, religious topics require extra care

5.3 Overall Risk Level

Based on the combination of:

- **Low to Medium** likelihood of access
- **Variable** (typically Low-Medium) impact
- **Partial** effectiveness of supplementary measures (contractual commitments have limited enforceability against US surveillance laws)

We assess the overall transfer risk as **Acceptable** with current safeguards in place for typical academic and market research applications. For sensitive research topics, customers should conduct their own transfer impact assessments.

6 Supplementary Measures

6.1 Technical Measures

The following technical measures reduce transfer risks:

6.1.1 Encryption

- All data transmitted to AI providers uses TLS encryption
- Data at rest in our EU infrastructure is encrypted
- No unencrypted data leaves the EEA

6.1.2 Transient Processing

- AI providers process data in memory for classification
- Data not used for model training
- AI providers may retain request logs for abuse detection (up to 30 days per their API terms)

6.1.3 Data Minimization

- Only survey response text and necessary context is transmitted
- Customer metadata (account info, billing) never leaves the EU
- Coding guides contain category definitions, not personal data

6.2 Contractual Measures

6.2.1 Standard Contractual Clauses

We have executed EU SCCs (Commission Decision 2021/914) with both AI providers:

- Module Two (Controller to Processor) applies
- Both providers commit to notifying us of government access requests
- Right to audit compliance included

6.2.2 Data Processing Agreements

- Explicit prohibition on using data for training
- Commitment to transient processing only
- Security obligations and incident notification requirements

6.2.3 Notification Commitments

Both providers commit to:

- Notifying us of any legally binding data disclosure request (to the extent legally permitted)
- Challenging overbroad or inappropriate requests
- Providing only the minimum data legally required

Note: These contractual commitments provide additional protection but cannot override US surveillance laws such as FISA Section 702. The practical enforceability of commitments to challenge or notify is limited by legal constraints.

6.3 Organizational Measures

6.3.1 Vendor Assessment

We conduct regular assessments of our AI providers including:
- Review of security certifications (SOC 2)
- Monitoring of subprocessor changes
- Annual contract review and renewal assessment

6.3.2 Customer Guidance

We advise customers to:
- Minimize personal data in survey responses where possible
- Consider anonymization before upload for sensitive surveys
- Avoid special category data (Article 9 GDPR) unless strictly necessary

6.3.3 Incident Response

We maintain incident response procedures including:
- Notification of customers if a provider reports government access
- Evaluation of whether to suspend transfers
- Documentation and regulatory notification where required

7 Conclusion

7.1 Assessment Summary

This Transfer Impact Assessment concludes that:

1. **Transfers to OpenAI and Anthropic are lawful** when conducted under the EU Standard Contractual Clauses with supplementary measures in place.
2. **The risk of problematic government access is low to medium** for typical research data, though contractual safeguards have limited enforceability against US surveillance laws.
3. **Supplementary measures provide partial mitigation** but cannot fully address Schrems II gaps due to the legal authority of US agencies. Risk assessment is based primarily on data characteristics (transient processing, academic focus) rather than contractual enforceability.
4. **Ongoing monitoring is required** to ensure continued adequacy as the US legal framework evolves.
5. **For sensitive research topics**, customers should conduct their own transfer impact assessments.

7.2 Recommendations

1. **Continue current arrangements** with OpenAI and Anthropic under SCCs with current supplementary measures.
2. **Monitor DPF certifications**: If either provider becomes DPF-certified, evaluate switching to that mechanism.
3. **Update this assessment annually** or upon material changes to:
   - US surveillance law
   - Provider policies or architecture
   - EU regulatory guidance

- Data transfer patterns

4. **Maintain customer guidance** on data minimization and avoiding unnecessary personal data in uploads.

8 Review Schedule

This assessment will be reviewed:

- **Annually**: Full review scheduled for January 2027
- **Upon material changes**: Including changes to US law, provider policies, or EU guidance
- **Upon request**: By customers or supervisory authorities

Document Control

Prepared by	AI Research & Technology Lab GmbH
Date	January 2026
Version	1.0
Classification	Internal / Customer Available
Next Review	January 2027

End of Transfer Impact Assessment