TRANSFER IMPACT ASSESSMENT: AMAZON WEB SERVICES

This Transfer Impact Assessment (TIA) evaluates the risks associated with transferring personal data to Amazon Web Services (AWS) as a sub-processor for DeepL SE. Following the Schrems II ruling and the 2023 adoption of the EU-U.S. Data Privacy Framework (DPF), this document confirms that adequate safeguards are in place to protect the rights of data subjects when using DeepL's neural translation services. This TIA is conducted in accordance with GDPR Articles 45 and 46, European Data Protection Board (EDPB) Recommendations 01/2020, CNIL Practical Guide on Transfer Impact Assessment (January 2025), and AWS GDPR Center compliance documentation.

Question	Response		
Know Your Transfer	**Data Flow Mapping:**		
	1. User submits text/document via DeepL interface *2. Data transmitted to DeepL SE servers (Germany)* *3. DeepL processes data using AWS infrastructure (EU-Central-1, Frankfurt)* *4. Translated output returned to user* *5. Data deleted from memory (Pro users)*		
	Transfer Characteristics:		
	Controller:	*Your Organisation*	
	Processor:	*DeepL SE (acting as Data Exporter in Germany)*	
	Sub-processor:	*Amazon Web Services, Inc. (acting as Data Importer in United States)*	
	Nature of Data:	*Text strings, documents, and metadata (IP addresses, account IDs)*	
	Data Subjects:	*Employees, customers, business contacts*	
	Purpose:	*Neural machine translation services*	
	Volume:	*Variable, based on usage*	
	Frequency:	*Real-time, per-request basis*	
	Duration:	*Milliseconds (in-memory processing)*	
	Sensitivity:	*May include business-confidential or personal information*	
	Retention Period:	*Zero retention for Pro users (in-memory processing only)*	
	Transfer Scenario:		
	Data is sent from the EU/EEA to DeepL. While DeepL is based in Germany and processes data in AWS Frankfurt (EU-Central-1), AWS is a U.S.-		Potential U.S. government access under the CLOUD Act.
			AWS's dual role as processor (inc. sub-processor) and (in some contexts) controller.

February 2026

TRANSFER IMPACT ASSESSMENT: AMAZON WEB SERVICES

Question	Response	
	headquartered company. This constitutes a "transfer" under certain legal interpretations due to:	Remote access possibilities by U.S.-based AWS personnel.
Identify The Transfer Tool	**Primary Transfer Mechanism:** • EU-U.S. Data Privacy Framework (DPF) - Adequacy Decision under GDPR Art. 45. • AWS (Amazon.com, Inc.) certified under DPF since July 2023. • Adequacy decision provides legal presumption of "essentially equivalent" protection. **Secondary Safeguards:** • AWS incorporates Standard Contractual Clauses (SCCs) - Updated June 2021 version, into service terms. • Supplementary Addendum to AWS GDPR DPA. **AWS GDPR Commitments:** • All AWS services shall process personal data in compliance with GDPR. • 500+ security and compliance features. • Customer data control: geographic storage selection, encryption options, access management. • Adherence to CISPE Data Protection Code of Conduct. **Legal Basis:** • Processing: Art. 6(1)(b) GDPR (Performance of Contract) for the translation service • Transfer: Art. 45 GDPR (Adequacy Decision) for the international transfer to a DPF-certified entity (AWS)	
Evaluation of Destination Country: United States of America	**Legal Framework:** The U.S. does not have a single federal data protection law equivalent to GDPR. Data protection is governed by sectoral laws and state-level regulations. **Surveillance Risks:** • Section 702 of the FISA (Foreign Intelligence Surveillance Act) allows U.S. authorities to request access to data held by U.S. companies for national security purposes • Executive Order 12333 authorizes government surveillance activities • CLOUD Act allows U.S. law enforcement to compel data disclosure **Adequacy Status:** The EU-U.S. Data Privacy Framework (DPF) was adopted in July 2023. AWS (Amazon.com, Inc.) is certified under the DPF, which significantly lowers the risk profile for this transfer compared to previous years. The	

TRANSFER IMPACT ASSESSMENT: AMAZON WEB SERVICES

Question	Response
	European Commission has issued an adequacy decision for the DPF, meaning data transfers to DPF-certified entities are deemed to provide protection "essentially equivalent" to the EU.
	DPF Safeguards:
	• Enhanced redress mechanisms for EU data subjects • Limitations on U.S. government access (proportionality requirements) • Independent oversight through Data Protection Review Court • Annual recertification requirements for U.S. companies
	Residual Risks:
	Despite the adequacy decision, residual risks remain: • DPF could be invalidated (as Schrems I and II invalidated previous frameworks) • FISA 702 and EO 12333 still authorize government data access • CLOUD Act allows U.S. law enforcement to compel data disclosure
	Risk Assessment:
	These residual risks are substantially mitigated by DeepL's technical architecture (see Step 4: Supplementary Measures).
	Effectiveness of Transfer Tool:
	The combination of DPF adequacy and SCCs provides a robust legal framework. The adequacy decision means that additional assessments beyond standard due diligence are not strictly required, but this TIA provides additional assurance given the potential for future legal challenges.
Identify and Adoption of Supplementary Measures	**Technical Safeguards Implemented by DeepL & AWS:**
	Encryption in Transit
	• Data is transmitted via TLS (Transport Layer Security) 1.2 or higher, ensuring protection against interception
	Encryption at Rest
	• Any data stored on AWS servers is encrypted with industry-standard AES-256
	Zero-Retention (Pro)
	• For DeepL Pro users, texts are processed in-memory and deleted immediately after translation • Minimizes the "window of risk" for surveillance

February 2026

TRANSFER IMPACT ASSESSMENT: AMAZON WEB SERVICES

Question	Response
	AWS Nitro System
	• Hardware-level isolation and confidential computing capabilities • Physically prevents AWS employees from accessing data during translation execution • Enhanced isolation that makes remote access technically infeasible
	Service Control Policies (SCPs)
	• DeepL utilizes AWS regional restrictions • Ensures data stays within designated EU regions
	External Key Store (XKS)
	• Option to hold encryption keys outside AWS cloud entirely • Renders data unreadable even if physically seized by authorities
	IAM Access Controls
	• Fine-grained permissions and credentials • Limits who can access data within AWS
	Contractual and Legal Safeguards:
	AWS Supplementary Addendum
	• Mandatory redirection of government data requests to the customer first • Explicit commitment to challenge any government request that is overbroad or conflicts with EU law (e.g., requests violating GDPR Art. 48) • Minimum disclosure warranty - if all legal challenges fail, AWS will only disclose the absolute minimum amount of data required by law
	Challenge of Unlawful Requests
	In the event AWS or DeepL receives a legally binding order from a public authority in a third country (e.g., a FISA request) for the disclosure of personal data, the Processor shall: • Use all reasonable legal efforts to challenge the request based on its lack of compatibility with EU law (GDPR) • Seek an interim injunction to suspend the effect of the order until a competent court has decided on the merits • Disclose only the absolute minimum amount of data necessary to comply with a finalized, non-appealable order.

February 2026

TRANSFER IMPACT ASSESSMENT: AMAZON WEB SERVICES

Question	Response
	Transparency & Notification
	Unless legally prohibited by the requesting authority (e.g., via a "gag order"), the Processor shall immediately notify the Data Exporter of any such request to allow the Exporter to seek a protective order or other appropriate remedy.
	Audit Rights
	The Processor shall provide the Data Exporter, upon request, with executive summaries of its SOC 2 Type II or ISO 27001 audit reports to verify that the technical measures described are operational and effective on the AWS infrastructure used.
	Organizational Measures:
	Data Minimization
	DeepL strips metadata where possible before processing, further reducing the "identifiability" of the data being transferred
	Localized Data Sovereignty
	By maintaining infrastructure primarily within the European Union (Germany), DeepL ensures that innovation speed is governed by the strict legal protections of the GDPR
	Dual Role Transparency
	AWS clarifies processor vs. controller roles for clear accountability
Measures and Procedural Steps Implemented	**Contractual Documentation**
	• Ensure DPA with DeepL references AWS as sub-processor • Verify SCCs are incorporated into service agreement • Request copy of AWS Supplementary Addendum • Confirm DPF certification status annually
	Technical Configuration
	• Configure DeepL account as "Pro" tier (zero-retention) • Enable encryption options where available • Document data minimization practices (avoid special category data)
	Organizational Measures

February 2026

Question	Response
	• Train users on appropriate use (no health data, sensitive personal data) • Establish incident response procedures • Designate responsible party for TIA monitoring • Document data flows in Article 30 processing register
	Documentation and Record-Keeping
	• Maintain this TIA document with DPA records • Record AWS/DeepL security notifications • Archive audit reports and certifications
	User Guidelines
	• Implement data classification policies • Establish approval workflows for sensitive data processing
	Incident Response
	• Define procedures for data breach notifications • Establish escalation paths for government access requests • Document communication protocols with DeepL/AWS
	Verification and Monitoring
	• Regular review of AWS DPF certification status • Monitor EDPB and local authority (inc. ICO & CNIL) guidance updates • Track AWS and DeepL security advisories • Review audit reports when available
Reassess at Intervals	**This TIA shall be reviewed:**
	• Annually (minimum requirement) • Upon regulatory change (e.g., DPF invalidation, new adequacy decisions) • Upon service change (AWS infrastructure changes, new sub-processors) • Upon incident (data breach, government access request)
	Monitoring Triggers:
	• Changes to U.S. surveillance laws (FISA, CLOUD Act amendments) • AWS or DeepL security incidents • EDPB or CNIL guidance updates

February 2026

Question	Response
	• DPF recertification outcomes • Court rulings affecting data transfers (potential Schrems III, etc.) • Changes to AWS service terms or DPA • DeepL architecture or processing location changes • New sub-processors added by DeepL or AWS
	Responsible Party:
	DeepL Privacy Team
	Review Sources:
	CNIL guidance emphasizes that sources used for assessment must be relevant, objective, reliable, verifiable, and publicly available. Key sources include: • AWS GDPR Center updates (https://aws.amazon.com/compliance/gdpr-center/) • DeepL privacy policy changes • EDPB recommendations and guidelines • National DPA enforcement actions • EU-U.S. DPF annual reviews • Court decisions from CJEU and national courts • Academic and expert analysis of data transfer mechanisms
	Documentation Requirements:
	• Maintain version history of TIA assessments • Document rationale for any changes to risk determinations • Record new supplementary measures adopted • Archive superseded versions for audit trail
	Next Scheduled Review:
	February 2027 (or sooner if triggered by events listed above)

February 2026