Privacy Policy for Adapt Global

Effective Date: January 1, 2025
Last Updated: July 7th, 2025

Introduction

Adapt Global Studios Inc. (d/b/a “Adapt” or "AdaptGlobal," "we," "us," or "our") is committed to protecting the privacy and confidentiality of personal data collected through our corporate website (adaptglobal.io) and our managed localization platform, Nuance. This Privacy Policy describes how we collect, use, disclose, transfer, and protect personal information in connection with our entertainment content localization services.

Our Business: We provide managed localization services for entertainment content, creating audio dubs and timed text assets for movies, television shows, and other entertainment media. We serve customers globally who send us content for localization, and we work with freelance translators, voice actors, and other specialists worldwide to deliver localized entertainment assets.

Global Operations: As a US-based company serving customers and working with freelancers internationally, we process personal data across multiple jurisdictions and comply with applicable privacy laws worldwide, including the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other relevant data protection frameworks.

Data Privacy Framework Compliance: Adaptglobal.io adheres to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. We are committed to subjecting all personal data received from European Union (EU) member countries, and the United Kingdom in reliance on the applicable Data Privacy Framework to the Framework's applicable Principles. To learn more about the Data Privacy Framework program, please visit: https://www.dataprivacyframework.gov/

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Adapt Global Studios Inc. commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner’s Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

What Personal Information We Collect

Customer Data

Business Contact Information:

- Names, job titles, and company affiliations
- Email addresses, phone numbers, and business addresses
- Account credentials and authentication information

Project and Content Data:

- Film and television show titles, synopses, and metadata
- Entertainment content files (video, audio, script files)
- Project specifications, deadlines, and delivery requirements
- Communication records related to projects
- Payment and billing information

Freelancer and Contractor Data

Professional Profile Information:

- Full name, professional pseudonyms, and stage names
- Contact details (email, phone, mailing address)
- Languages spoken and proficiency levels
- Professional qualifications, experience, and portfolio samples
- Performance ratings and work history on our platform

Onboarding and Compliance Data:

- Tax identification numbers and forms (W-9, 1099, international equivalents)
- Banking information for payment processing
- Identity verification documents
- Work authorization and visa status (where applicable)
- Background check results (where legally required)

Work Product and Performance Data:

- Completed translations, voice recordings, and localized content
- Quality assessments and performance evaluations
- Time tracking of work related tasks and project completion data
- Communication records with our team and customers

Website and Platform Users

Technical Data:

- IP addresses, browser type, and device information
- Website usage patterns and page views
- Login times and platform usage analytics
- Cookies and tracking technology data

Account Data:

- User profiles and preferences
- Support ticket information and communications
- Marketing preferences and communication history

How We Use Personal Information

Lawful Bases for Processing (GDPR)

- **Contract Performance:** Processing necessary to perform our localization services contracts
- **Legitimate Interests:** Business operations, service improvement, and fraud prevention
- **Legal Compliance:** Meeting tax, regulatory, and legal obligations
- **Consent:** Where specifically obtained for marketing or optional services

Primary Use Purposes

Service Delivery:

- Managing and executing localization projects
- Coordinating between customers and freelancers
- Quality assurance and project management
- Delivering completed localized entertainment assets

Business Operations:

- Processing payments and managing accounts
- Providing customer support and technical assistance
- Maintaining and improving our platform and services
- Analysing usage patterns to enhance user experience

Legal and Compliance:

- Complying with tax reporting and financial regulations
- Meeting entertainment industry confidentiality requirements
- Responding to legal requests and protecting our rights
- Conducting background checks where legally required

Communications:

- Sending service-related notifications and updates
- Marketing our services (with appropriate consent)
- Providing customer support and responding to inquiries
- Sharing important policy or service changes

Information Sharing and Disclosure

With Customers

We share freelancer work product and relevant project information with customers as necessary to deliver localized entertainment assets. This includes completed translations, voice recordings, and quality assessments.

With Freelancers and Contractors

We provide project details, content files, and customer specifications to freelancers as necessary for them to complete localization work. We maintain strict confidentiality agreements with all freelancers handling entertainment content.

With Service Providers

We work with trusted third-party service providers who assist with:

- **Cloud hosting and data storage** (AWS)
- **Payment processing** (Stripe, Wise, international banking partners)
- **Communication tools** (email services, video conferencing platforms)
- **Analytics and website functionality** (website analytics, customer support tools)
- **Background check services** (where legally required for freelancer onboarding)

All service providers are bound by comprehensive data processing agreements and implement appropriate security measures.

Legal Disclosures

We may disclose personal information when required by law or when we have a good faith belief that disclosure is necessary to:

- Comply with legal process, court orders, or regulatory requirements
- Protect our rights, property, or safety, or that of our users or others
- Investigate potential violations of our terms of service
- Respond to emergency situations involving threats to personal safety

Business Transfers

In the event of a merger, acquisition, or sale of all or part of our business, personal information may be transferred as part of that transaction, subject to appropriate confidentiality protections.

International Data Transfers

Cross-Border Transfer Framework

As a global entertainment localization service, we regularly transfer personal data across international borders. We implement appropriate safeguards for all international transfers:

Data Privacy Framework Participation: Adaptglobal.io participates in and has certified its compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), and the UK Extension to the EU-U.S. DPF. We are committed to subjecting all personal data received from the EU, and UK in reliance on the applicable DPF to the DPF Principles.

For EU/EEA Personal Data:

- **EU-US Data Privacy Framework:** We are self-certified under the EU-US DPF for transfers to the United States
- **Standard Contractual Clauses:** We use EU-approved SCCs for transfers to countries without adequacy decisions
- **UK Extension:** Our DPF certification extends to UK personal data transfers

For Other Jurisdictions:

- We conduct Transfer Impact Assessments to evaluate the adequacy of protection in destination countries
- We implement supplementary measures where local laws may undermine transfer safeguards
- We maintain comprehensive documentation of all transfer mechanisms and safeguards

Entertainment Content Considerations

Given the confidential nature of entertainment content, we implement enhanced security measures for cross-border transfers:

- Encryption for all content files in transit
- Secure file transfer protocols and access controls
- Comprehensive confidentiality agreements with international freelancers
- Monitoring and audit trails for all content access and transfers

---

Data Retention

Retention Principles

We retain personal information only as long as necessary for the purposes outlined in this Privacy Policy and as required by applicable law.

Customer Data:

- **Active Projects:** Throughout project duration plus 3 years for warranty and support
- **Completed Projects:** 7 years for business records and tax compliance
- **Marketing Data:** 3 years from last interaction or until opt-out

Freelancer Data:

- **Active Contractors:** Throughout working relationship plus 3 years
- **Performance Records:** 5 years for reference and quality assurance
- **Tax Documents:** 7 years as required by US tax law
- **Identity Verification:** Securely destroyed after verification complete

Entertainment Content:

- **Client Content Files:** Retained as specified in individual client agreements
  Work Product: Retained as specified in individual client agreements
- **Confidential Materials:** Handled according to specific confidentiality agreement terms

Automated Deletion

We implement automated systems to delete personal information in accordance with our retention schedules. Users may request earlier deletion subject to legal and contractual obligations.

Data Security

Security Measures

We implement comprehensive technical and organizational security measures to protect personal information:

Technical Safeguards:

- Encryption for data in transit and at rest
- Multi-factor authentication for all system access

- Regular security monitoring and intrusion detection
- Secure cloud infrastructure
- Regular security testing and vulnerability assessments

Organizational Measures:

- Comprehensive staff training on data protection and confidentiality
- Role-based access controls limiting data access to authorized personnel
- Background checks for employees handling sensitive data
- Regular security audits and compliance assessments
- Incident response procedures and breach notification protocols

Entertainment Industry Standards:

- Compliance with TPN and Motion Picture Association (MPA) Content Security Best Practices
- Secure workflows for confidential creative materials

Breach Notification

In the event of a personal data breach, we will:

- **Assess Impact:** Evaluate risks to individuals within 24 hours
- **Notify Authorities:** Report to relevant supervisory authorities within 72 hours where required
- **Inform Individuals:** Notify affected individuals without undue delay for high-risk breaches
- **Document Incident:** Maintain comprehensive records of all breaches and response actions

---

Your Privacy Rights

Universal Rights

All users have the following rights regarding their personal information:

Access: Request information about what personal data we collect and how we use it
Correction: Request correction of inaccurate or incomplete personal information
Deletion: Request deletion of personal information (subject to legal and contractual limitations)
Portability: Receive personal data in a structured, machine-readable format
Restriction: Request limitation of processing in certain circumstances
Objection: Object to processing based on legitimate interests or for marketing purposes

Jurisdiction-Specific Rights

For EU/EEA and UK Residents (GDPR/UK GDPR):

- Right to withdraw consent where processing is based on consent
- Right to lodge complaints with supervisory authorities
- Right to object to automated decision-making and profiling

For California Residents (CCPA/CPRA):

- Right to know what personal information is collected, used, and shared
- Right to delete personal information
- Right to opt-out of sale or sharing of personal information for targeted advertising
- Right to limit use of sensitive personal information
- Right to non-discrimination for exercising privacy rights

For Other US State Residents: Similar rights are available under Virginia CDPA, Colorado CPA, Connecticut CTDPA, and other applicable state privacy laws.

Exercising Your Rights

To exercise your privacy rights:

Email: privacy@adaptglobal.io
Phone: +1 (844) 523-2784
Mail: Adapt Global Studios Privacy Team
1905 Sherman Street
Ste 200 #1791
Denver, CO 80203
United States

We will respond to rights requests within 30 days (up to 90 days for complex requests) and may require identity verification for security purposes.

Cookies and Tracking Technologies

Types of Cookies We Use

Essential Cookies: Necessary for website and platform functionality, including:

- Authentication and security
- User preferences and settings
- Shopping cart and session management

Analytics Cookies: Help us understand website usage and improve our services:

- Google Analytics (with privacy-enhanced settings)
- Website performance monitoring
- User behaviour analysis

Marketing Cookies: Used for advertising and marketing purposes:

- Targeted advertising and retargeting
- Social media integration
- Email marketing tracking

Your Cookie Choices

EU/EEA and UK Users: We obtain explicit consent before placing non-essential cookies. You can manage your preferences through our cookie banner or privacy settings.

California and Other US Users: You can opt-out of targeted advertising cookies through the "Do Not Sell or Share My Personal Information" link in our website footer. We honor Global Privacy Control (GPC) signals.

Browser Settings: You can also control cookies through your browser settings, though this may affect website functionality.

Children's Privacy

Our services are not directed at children under 13, and we do not knowingly collect personal information from children under 13. If we discover we have collected personal information from a child under 13, we will delete it promptly.

Some entertainment content we localize may include performances by minors. In such cases, we implement additional safeguards including parental consent verification and enhanced data protection measures as required by applicable law.

Regional Privacy Information

California Residents

Categories of Personal Information Collected: Identifiers, professional information, commercial information, internet activity, and payment information as described above.

Business Purpose: We use personal information for service provision, business operations, legal compliance, and communications as outlined in this policy.

Third-Party Sharing: We do not sell personal information. We share information with service providers, customers (work product only), and as required by law.

Your Rights: Access, deletion, correction, portability, opt-out of targeted advertising, and non-discrimination.

EU/EEA and UK Residents

Data Controller: AdaptGlobal.io, Inc. serves as the data controller for personal information processed in connection with our services.

Lawful Basis: We process personal information based on contract performance, legitimate interests, legal compliance, and consent as applicable.

Data Protection Officer: For questions about data protection, contact: dpo@adaptglobal.io

Supervisory Authority: You have the right to lodge complaints with your local data protection authority.

Canadian Residents

We comply with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial privacy laws, including Quebec's Law 25. Canadian residents have rights of access, correction, and complaint to the Office of the Privacy Commissioner of Canada.

APAC Residents

We are committed to complying with applicable privacy and data protection laws across the Asia-Pacific (APAC) region, including but not limited to India's Digital Personal Data Protection Act (DPDP), Hong Kong's Personal Data (Privacy) Ordinance (PDPO), and South Korea's Personal Information Protection Act (PIPA).

Categories of Personal Information Collected: Identifiers, contact details, professional and transactional information, internet activity, and other data necessary to provide our services.

Purpose of Use: We collect and process personal information for service delivery, customer support, business operations, legal compliance, and marketing communications, in accordance with local legal requirements.

Cross-Border Transfers: Where personal information is transferred across borders, we ensure appropriate safeguards are in place in compliance with relevant data transfer regulations, including obtaining consent where required.

Your Rights: Depending on your jurisdiction, you may have rights to access, correct, delete, or object to the processing of your personal information. You may also have the right to withdraw consent or lodge a complaint with your local privacy authority.

Third-Party Services and Links

Our website and platform may contain links to third-party websites and services. This Privacy Policy does not apply to these external sites. We encourage you to review the privacy policies of any third-party services you use.

We integrate with various third-party services for business operations, including payment processors, cloud storage providers, and communication tools. These integrations are governed by comprehensive data processing agreements ensuring appropriate data protection.

Updates to This Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our practices, services, or applicable law. We will:

- Post the updated policy on our website with a new "Last Updated" date
- Notify users of material changes via email or prominent website notice
- For users with accounts, provide notice through the platform dashboard
- Maintain archives of previous policy versions

Continued use of our services after policy updates constitutes acceptance of the revised terms.

Contact Information

Privacy Team

Email: privacy@adaptglobal.io
Phone: +1 (844) 523-2784
Mail: Adapt Global Studios Privacy Team
1905 Sherman Street
Ste 200 #1791
Denver, CO 80203
United States

Data Protection Officer (EU/UK)

Email: dpo@adaptglobal.io

General Business Inquiries

Email: info@adaptglobal.io
Website: https://adaptglobal.io

Dispute Resolution

If you have concerns about our privacy practices that we cannot resolve directly, you may:

- File complaints with relevant supervisory authorities
- Contact consumer protection agencies in your jurisdiction
- For EU residents: Contact your local Data Protection Authority
- For California residents: Contact the California Privacy Protection Agency

---

Legal Framework and Compliance

This Privacy Policy is designed to comply with:

- EU General Data Protection Regulation (GDPR)
- UK Data Protection Act 2018 and UK GDPR
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Connecticut Data Privacy Act (CTDPA)
- Other applicable US state privacy laws
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australia Privacy Act 1988
- Entertainment industry confidentiality and security standards

DPF Accountability and Enforcement

Adapt Global Studios Inc. is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Adapt Global Studios Inc. commits to resolve complaints about our collection or use of personal data transferred to the United States pursuant to the DPF Principles.

In cases of onward transfers to third parties, Adapt Global Studios Inc. remains liable under the DPF Principles if those parties process personal data in a manner inconsistent with the Principles, unless we can demonstrate that we were not responsible for the event giving rise to the damage.

Under certain conditions, individuals may invoke binding arbitration for unresolved complaints under the DPF Principles, after all other available dispute resolution mechanisms have been exhausted. Details on this process are available in Annex I of the DPF Principles: https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction.

Last Review: This policy was last comprehensively reviewed and updated on June 30th, 2025, to ensure compliance with current privacy laws and industry best practices.

This Privacy Policy is effective as of January 1, 2025. For questions about this policy or our privacy practices, please contact our Privacy Team using the information provided above.