

INTERPRETERCONNECT

PRIVACY POLICY

All Languages is committed to protecting your privacy in a variety of ways, including using industry-accepted security measures to protect against the loss, misuse, and alteration of data contained in our system. This Privacy Policy applies to all of the interpretation and translation services offered through our call centre. Our policy is designed to ensure the safety and accuracy of our clients' and their customers' personal information. Any information revealed to us will never be sold, rented, traded, or leased. We adhere to all HIPAA Administrative Simplification Regulations found at 45 CFR 160, 162, and 164. All employees and independent contractors are required to complete the requisite training courses upon onboarding and annually thereafter.

Our call centre complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), as set forth by the U.S. Department of Commerce. Our call centre has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Our call centre has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, our call centre commits to refer 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 and the Swiss-U.S. DPF to JAMS, an alternative dispute resolution provider based in the United States. Contact your Account Manager to bring the complaint to our attention. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit <https://www.jamsadr.com/dpf-dispute-resolution> for more information or to file a complaint. The services of JAMS are provided at no cost to you. Under certain conditions, individuals have the right to invoke binding arbitration under the Data Privacy Framework (DPF). This arbitration option is available as a last resort mechanism for addressing unresolved complaints regarding an organization's compliance with the DPF Principles.

Our call centre continues to monitor and apply applicable changes from compliance with current and developing state privacy laws, such as the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act (VCDPA), and the Utah Consumer Privacy Act (UCPA).

CONFIDENTIALITY PRECAUTIONS

Each and every person who works with our call centre, either as a direct employee or as a contract interpreter, receives training in the compliance with confidentiality and nondisclosure laws. This training takes place prior to

the employee or contractor ever working with the customer in any form. Further, questions pertaining to their understanding of this information are incorporated into our testing program. Periodic review of this information takes place via quarterly training updates. As part of our employee initiation program, every employee is required to read, understand, and sign our proprietary employee manual, which includes all documentation that supports confidentiality, HIPAA, and Data Privacy Framework requirements.

Our call centre is constantly aware of the necessity to keep all documentation and recordings regarding our customers and their clients in strict confidentiality. We have implemented the following procedures to ensure that our practice of protecting private information is followed. These practices are consistently reviewed and updated and include:

- Strict guidelines require that customers' confidential information never leave our secure office.
- No confidential information is available on the web. All data is stored securely in-house.
- Our premises are not open to the public; the doors are locked and solely accessible via regulated key cards.
- Every employee has a strict confidentiality agreement with emphasis on HIPAA and Data Privacy Framework compliance.
- Interpreters are bound by signed confidentiality and HIPAA compliance agreements.

In order to provide our services, we may collect the following types of information:

- **Information you provide** — When you sign up for services with us, we ask you for personal information (such as your name, email address, phone number, other account information, and an account password). For certain accounts, we accept credit card or other payment account information that we maintain in encrypted form on secure servers.
- **User communications** — When you send email or other communications, we may retain those communications in order to process your inquiries, respond to your requests, and improve our services.

PERSONAL INFORMATION

When you sign up for our interpreter services, the only confidential information that is necessarily exchanged is the information that the interpreter is relaying between the two parties.

Our call centre does record some telephone interpreting calls with permission from our customers. These recordings are made strictly for internal quality assurance purposes and are securely retained for 90 days, at which point they are destroyed.

- Call recordings are encrypted with an encryption level of at least 256 AES.
- Access to call recordings is limited to authorized staff.
- Recordings are kept securely on the premise only.

Our call centre customizes services to meet the needs of our customers. We will gather any information that you require for billing purposes and this information will appear on the invoices. We will not collect or use sensitive information for purposes other than those described in this Privacy Policy and/or in the supplementary service privacy notices.

Upon request, we will provide you with information on whether we hold, or process on behalf of a third party, your personal information. To request this information, please contact your Account Manager. When notified by email or mail, we will make reasonable effort to correct, amend, or delete such personal data if such data is demonstrated to be inaccurate or incomplete.

INFORMATION SHARING

Our call centre only shares personal information with other companies or individuals outside of the company in the following limited circumstances:

- We have your consent. We require **opt-in consent** for the sharing of any sensitive personal information.
- We have a good faith belief that access, use, preservation, or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process, or enforceable governmental request; (b) enforce applicable Terms of Service, including investigation of potential violations thereof; (c) detect, prevent, or otherwise address fraud, security, or technical issues; or (d) protect against imminent harm to the rights, property, or safety of our staff, its users, or the public as required or permitted by law.

If we become involved in a merger, acquisition, or any form of sale of some or all of its assets, we will provide notice before personal information is transferred and becomes subject to a different Privacy Policy.

INFORMATION SECURITY

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure, or destruction of data. These include internal reviews of our data collection, storage, and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data.

We restrict access to personal information to employees, contractors, and agents who need to know that information in order to operate, develop, or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations. Additionally, our call centre maintains current certification for compliance with PCI data security standards.

DATA INTEGRITY

Our call centre processes personal information only for the purposes for which it was collected and in accordance with this Privacy Policy or any applicable service-specific privacy notice. We regularly review our data collection, storage, and processing practices to ensure that we only collect, store, and process the personal information needed to provide or improve our services.

ENFORCEMENT

Our call centre is responsible for the processing of personal data it receives, under the Data Privacy Framework, and subsequently transfers to a third party acting as an agent on its behalf. Our call centre complies with the Data Privacy Framework for all onward transfers of personal data from the EU, UK, and Switzerland, including the

onward transfer liability provisions. With respect to personal data received or transferred pursuant to the Data Privacy Framework, our call centre is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, our call centre may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Our call centre regularly reviews its compliance with this Privacy Policy to ensure it meets both HIPAA and Data Privacy Framework standards. When we receive formal written complaints, it is our call centre's policy to promptly contact the complaining user regarding his or her concerns. We will cooperate with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between our call centre and an individual.

CHANGES TO THIS PRIVACY POLICY

Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent, and we expect most such changes will be minor. Regardless, we will post any Privacy Policy changes on our website and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification) of Privacy Policy changes.

If you have any additional questions or concerns about this Privacy Policy, please feel free to contact your Account Manager.