Addressing the Translation Problem in Compliance

A traveler walking through the streets of New York City could hear nearly 800 different languages. In fact, 45 percent of New Yorkers speak a language other than English at home. For businesses serving these populations, and for global organizations everywhere, translation services fill a vital role. But businesses must also address the translation problem in compliance.

For example, HIPAA regulations mandate that organizations maintain confidentiality of protected health information (PHI). This means that they must protect PHI from unauthorized access at all stages, including in transit and in storage. That includes data being translated. Penalties for violating HIPAA regulations can cost organizations millions of dollars.

Employees and businesses have several translation options at their disposal. They can use a free online tool, such as Google Translate. Alternatively, they can take a step up and pay for machine translation, either online or on-premises. Finally, they can hire human translators. Each option has implications for compliance.

Option 1: Free Online Translation Services

Machine translation tools improve every day. Type a phrase into Google Translate, for example, and you have a relatively reasonable translation in a millisecond. However, many users fail to realize that they surrender control of their data once they enter it into the translation app.

At the very least, Google and other free machine translators use your data to help improve their translation services. This means that other people entering similar phrases into the translator may see your data. Worse, big chunks of the data could become available online. Even the possibility that this could happen violates many privacy laws.

Option 2: Paid Online Translation Services

In addition to free online translation services, many providers offer paid options. These services take much greater care with your data, promising not to store it on their servers or share it with other parties. In fact, Microsoft Translator announced in 2019 that it is certified compliant with ISO, HIPAA and SOC.

However, before using a paid translation service, be sure to check the details of the service's confidentiality agreements. For example, some services store the data you input for a few hours before deleting it. This could violate a strict privacy law.

Additionally, even if the online translation service certifies compliance, data may still prove vulnerable as it travels to and from the service. To be safe, ensure data encryption in transit and avoid public Wi-Fi.

Option 3: Offline Translation Programs

On-premises machine translation tools, while expensive, offer the highest degree of security. When organizations purchase translation software and install it on secure computers not connected to the internet, they retain control over sensitive data. As long as the company protects its local network and machines, the data remains safe from unauthorized access.

As a downside, an effective translation software will utilize artificial intelligence (AI). While AI greatly improves the translation, it requires more computing power. Additionally, deploying the solution will require personnel with working knowledge of AI programs.

Option 4: Human Translators

To avoid costly miscommunications, professional documentation must be accurate. Advancements in AI have vastly improved the abilities of machine translators. However, in some cases machines will prove unequal to the task of providing a translation with the necessary nuances. In these instances, human translators prove necessary.

When using human translators, organizations must choose their providers carefully. In addition to a working knowledge of industry-specific language, translators must also understand and accommodate compliance considerations.

Best Practices to Address the Translation Problem in Compliance

Regardless of which translation option they choose, organizations should follow several best practices to ensure data security.

- Avoid unsecured Wi-Fi and email for transferring sensitive data – Never transfer sensitive data to a machine or human translator over public Wi-Fi. Likewise, avoid transferring through email. Instead, use an encrypted online portal.
- Vet your translation provider – Carefully check any translation service before using them. Make sure they have established security practices in place that satisfy applicable regulations. For starters, look for ISO 27001 accreditation. Professional translators should also sign a non-disclosure agreement (NDA).
- Educate employees – Make sure employees understand both the privacy regulations that apply and the dangers of using free translation tools and public Wi-Fi. Provide a safe translation tool for them to use and build that use into the organization's data governance policies.

The data compliance experts at Messaging Architects can help you make sense of complex privacy regulations. Our consultants will provide a risk assessment and compliance monitoring as part of your overall data security and compliance strategy.