STP

stptrans.com
@STPConnect

Data security at STP

At STP, we take the security of client data very seriously. Much of the content we translate contains personal and business-sensitive data. Read on to find out what we do to make sure it stays secure.

Compliance and certifications

We comply with all national and international laws and regulations on the security of personal data and other data.

Our bespoke project management system allows us to track projects that may contain personal data and sensitive personal data so we can ensure that data is not retained in translation memories or distributed insecurely.

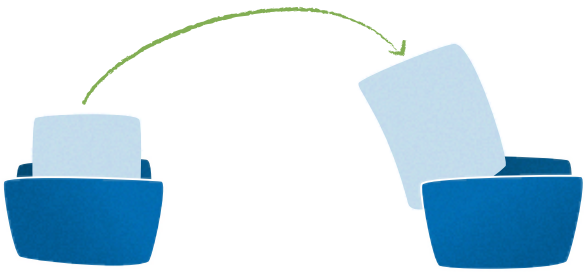
We may act as either a data controller or data processor depending on our relationship with you and the data you transmit to us.

- GDPR-compliant internal processes and project management system
- ISO 17100-certified procedures ensure traceability throughout the entire translation process
- Data processing agreements available if required

Secure file transfer

We minimise the transmission of files and sensitive data through less secure communication channels such as email, preferring to keep data contained within cloud-based CAT tools wherever possible.

Where file transfer via email is necessary, we use of password-protected ZIP files with AES-256 encryption.



Technology stack

Our organisation runs on virtual machines hosted on our own servers. This means we keep control of our data in-house and minimises the need to copy data onto local drives, significantly reducing the risk of data leaks.

We also host our own project management system and email server. We require the use of secure passwords and encourage employees to lock their screens when not in use. We roll out OS updates on our virtual and physical machines on a monthly basis.

For our remote workers, work involving client or personal data is not permitted over public wi-fi networks or in public locations such as cafés.

For more information, see stptrans.com/data-security