



STP Client Data Security Policy

Purpose of the Policy

Sandberg Translation Partners Ltd (STP) places great importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

This policy is for distribution to clients, outlining the responsibilities, workflows and processes in STP's dual role as:

- Data Controller responsible for collecting and retaining personal data for client contacts; and
- Data Processor responsible for the safe and secure handling, retention and further processing of content for translation, which may contain personal data.

This policy supplements STP's general GDPR Policy, available on our website at <http://stptrans.com/GDPR>.

Client contact data

We collect data from clients to enter into a contract to supply translation or other linguistic services, to carry out tasks as commissioned, and to ensure that we comply with our legal obligations. As such, STP has a contractual and/or legal obligation to collect this data.

The information we collect includes names, job titles and contact details for client vendor and project managers, accounts payable, and other contacts involved in the work we carry out for you, as well as bank and invoicing details.

This data is stored in our project management database, in email correspondence, and within our accounting and banking systems. It is only accessible to appropriate STP staff members.

Client data is retained indefinitely for contracts and agreements, in our accounts, and in our project management system. Emails are retained for a period of 7 years, after which they are deleted or destroyed.

Personal data in content for translation

STP recognises that the safe and secure handling of personal data in content for translation is of the utmost importance to our clients, your clients, and the data subjects whose data we process.

The following policy sets out our commitment to data protection obligations, and outlines our processes and workflows, which we will comply with unless we have signed a specific agreement with you to the contrary.

What we expect of you

As Data Controller or first-line Data Processor of content for translation, we expect you to:

- Have the data subject's consent for sending their data for translation or other processing;
- Notify us of any personal data in content for translation that hasn't already been removed or anonymised;
- If content does contain personal data, indicate whether it is sensitive or contains special categories of data, which should be considered high risk; and
- If content does contain personal data, indicate whether it can be sent outside of the EU/EEA/adequate countries for translation or other processing.

We will, additionally, support you in safeguarding personal data in content for translation by engaging our project managers and linguists in flagging up personal data in content for translation, even if its presence has not been indicated to us at the time of ordering.

Data processing agreements

We understand the importance of having a transparent, GDPR compliant data processing chain, which allows the Data Controller to track where and how their personal data is processed.

Should you so require, we can enter into a Data Processing Agreement with you, agreeing to specific data processing and retention requirements, especially when it comes to handling of sensitive personal data in content for translation. Complying with a specific data handling process or retention period will incur a small administration fee added to our invoice, to cover the cost of processing.

As a reputable, respected language service provider, however, we are confident that our data processing and retention policies, as outlined below, can be accepted "as is", as proof of reasonable and secure processes, fulfilling not only the requirements but also the sentiment of GDPR regulations.

Data profiling and retention

To ensure appropriate handling of content for translation, all incoming projects are profiled and categorised into the following three security categories, based on the information received and our own best understanding:

- No personal data
- Non-sensitive personal data
- Sensitive personal data

Each category carries different processing workflows and retention periods for content in translation, as follows, with sensitive personal data being retained for a minimal amount of time.

Content with no personal data

Processing and storage	Retention period
Internal project folders	7 years
Emails and email attachments	7 years
Translation Environment Tools	Indefinite unless otherwise agreed
External suppliers	No restrictions on retention or geographical location of linguist

Content with non-sensitive personal data

Processing and storage	Retention period
Internal project folders	7 years
Emails and email attachments	7 years
Translation Environment Tools	Indefinite unless otherwise agreed Data protected by restricting use to project TMs and client/account-specific TMs only Data retained in any other repositories cleaned of personal data
External suppliers	Deletion of content after delivery, no restriction on geographical location of linguists unless otherwise requested

Content with sensitive personal data

Processing and storage	Retention period
Internal project folders	6 months (provided that our invoice has been settled before this time)
Emails and email attachments	6 months (provided that our invoice has been settled before this time)
Translation Environment Tools	Max. 6 months, data retained in project TMs only
External suppliers	Deletion of content after delivery, content not transferred outside of EU/EEA/adequate countries without explicit agreement with the client

Translation Memories and Machine Translation Systems

Much of the work STP carries out for its clients is recurring. To ensure the continuity of the high translation quality we provide, and to remain consistent with our previous translations where we don't work in your own secure translation environment, we maintain translation memories for the following purposes:

- Project TMs connected to individual translation projects only;
- Client/end-client TMs used on specific accounts for an individual client only;
- Domain-specific reference TMs purged of personal data.

We also use content for translation produced at STP for training our proprietary machine translation engines, which we develop and deploy at our discretion and/or as per any agreements between us, to

be able to provide you with a competitive, sustainable service. Our MT processes are fully documented and our MTPE workflows are in line with the ISO 18587 machine translation post-editing standard to which we are certified.

Access and secure storage

At STP, content for translation is stored within:

- Secure network folders
- Translation Environment Tools hosted either on your or our servers, or installed on local computers
- Encrypted email attachments

Content for translation can only be accessed by relevant STP production staff, and it is subject to the above mentioned, or mutually agreed, retention periods.

Transfer of data

Content for translation is transferred between you, our client, STP, and our sub-processors using the below secure methods only:

- Your own secure translation environment
- Your own secure file transfer method
- Secure file transfer method hosted by STP
- Password-protected .zip attachments with AES-256 encryption

Sub-processing

Many of STP's projects are carried out by internal linguists, but we also maintain a pool of external suppliers, whom we subcontract work out to.

All sub-processors are vetted according to our vendor management policy and ISO 17100 translation services standard certified workflows. All of our sub-processors have contractually agreed to comply with the terms and conditions for processing data provided in their framework agreement with STP and our information security policy. These two documents further outline the external suppliers' role and responsibilities towards STP, our clients and the content they translate, including the safe and secure handling, storage and transfer of content which contains personal data.

STP takes full responsibility for the work carried out by its subcontractors.

Further information

Further information on STP's policies on the processing, transfer and storage of personal data, alongside the company's detailed processes, can be found in the following documents which we are happy to share with our clients upon request:

- *Terms & Conditions of Business*
- *Internal Information Security Policy*
- *Vendor Framework Agreement*
- *Vendor Information Security Policy*

STP reserves the right to update this policy at any point.