Sandberg's Data Security Policy

Document control

Version number:	2.2
Policy owner:	Adam Dahlström, IT Manager
Effective date:	25 May 2018
Last review date:	23 Jan 2024
Next review by date:	23 Jan 2025

Version control

Ver	Date	Changes
2.2	23 Jan 2024	Reviewed; no edits
2.1	21 Feb 2023	Reviewed; no edits
2.0	15 Feb 2022	Client Data Security and Data Classification policies merged
1.1	11 Jan 2022	Content revised, updated to follow a new policy template
1.0	25 May 2018	First version

Purpose

Sandberg Translation Partners Ltd (Sandberg) holds information that must be protected against unauthorised access, disclosure, modification or otherwise misuse. This policy is part of an overarching set of policies dealing with aspects related to data protection and information security at Sandberg, including the Data Protection/GDPR Policy, Information Security Policy, Access Control Policy, etc.

Sandberg 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 internal use as well as for distribution to clients, outlining the responsibilities, workflows, and processes in Sandberg'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 Sandberg's general GDPR Policy, available on our website at www.stptrans.com.

Scope

The Data Security Policy applies to all employees at Sandberg who handle data, regardless of source.

All Sandberg employees are required to read, understand, and comply with the Data Security Policy and to present any questions to the policy owner or to HR.

Outline

Internal data classification

Internal data is organised by means of classification and applicable handling methods. The following processes outline how data is inventoried, classified, labelled and handled with all the relevant steps and procedures for information security standards to be met and adhered to continuously. Unauthorised access to data or wrong classification of data could expose Sandberg to various risks such as legal and compliance issues, malicious attacks, or compromise of network systems and services, and others.

In order to protect data according to a level of sensitivity, it is foremost necessary for information assets to be identified. This includes identifying what classified information Sandberg has in possession and who is the information owner, i.e. who is responsible for it. Data can take different forms and types, such as:

- E-mail
- Electronic documents in various formats
- Information systems and database platforms
- Paper documents
- Offline storage devices
- Verbally transmitted information

Based on the data assessment and the created asset inventory, different values are applied to assets in the context of confidentiality, integrity, and availability. Sandberg assigns information classification standards in four (4) tiers and in two different ways. Standard data is classified as:

- Confidential – highest confidentiality level
- Restricted – medium confidentiality level
- Internal Use – lowest confidentiality level
- Public – public information and/or accessible on the public domain

Sandberg follows inspiration and guidance for the implementation and execution of the data classification policy as prescribed in ISO 27001, the global standard for information security management – controls outlined under sections A.8.1.1 through to A.8.2.3 within the ISO 27001 standard – as well as in accordance and full compliance with national and international regulations.

Data labelling is undertaken in different ways for the different forms and types of data, where for example electronic documents are subject to different rules compared to paper documents.

Each type of media is falling under different rules on how assets are being protected based on the confidentiality level assigned. For example, paper documents with a Confidential value are to be securely locked in a cabinet in the office with access to the cabinet only by users with the appropriate level of access.

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, Sandberg 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 clients, 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 Sandberg 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

Sandberg recognises that the safe and secure handling of personal data in content for translation is of the utmost importance to our clients, their clients in turn, 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 client agreement to the contrary.

What we expect of clients

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

- Have the data subject’s consent for sending their data for translation or other processing;
- Notify Sandberg 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 client 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.

Where clients so require, we can enter into a Data Processing Agreement, 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 may 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 Data protected by restricting use to project TMs and client/account-specific TMs only
External suppliers	Deletion of content after delivery, no restriction on geographical location of linguists unless otherwise requested

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
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 Sandberg 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 client-side 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.

We also use content for translation produced at Sandberg 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 clients 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 Sandberg, content for translation is stored within:

- Secure network folders
- Translation environment tools hosted either by clients or on Sandberg servers, or installed on local computers

- Encrypted and password-protected email attachments

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

Transfer of data

Content for translation is transferred between clients, Sandberg, and our sub-processors using the below security methods only:

- Client-side secure translation environments
- Client-initiated secure file transfer
- Secure file transfer method maintained by Sandberg
- Password-protected .zip attachments with AES-256 encryption

Sub-processing

Many of Sandberg'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 Sandberg and our information security policy. These two documents further outline the external suppliers' role and responsibilities towards Sandberg, our clients and the content they translate, including the safe and secure handling, storage and transfer of content which contains personal data.

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

Further information

Further information on Sandberg'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
- Information Security Policy
- Vendor Framework Agreement
- Vendor Information Security Policy

Compliance measurement

Deliberate or unintentional breaches of this policy will be considered a disciplinary matter. Such breaches under the disciplinary procedure may constitute gross misconduct and may lead to action up to and including dismissal.

Breaches of this policy must be notified to the policy owner for investigation.

Review & update

This policy is reviewed and updated annually. In cases where changes to the organisation or changes to national, international, GDPR or otherwise data security-related regulations take place, additional and more frequent reviews of the policy may take place.