Sandberg's GDPR Policy

Document control

Version number:	1.2
Policy owner:	Susan Hoare
Effective date:	May 2018
Last review date:	25 Jan 2024
Next review by date:	25 Jan 2025

Version control

Ver	Date	Changes
1.2	25 Jan 2024	Second version – update STP > Sandberg
1.0	1 May 2022	First version

Purpose and Scope

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 distribution to clients, employees and sub-contractors, and for the Information Commissioners Office, if requested, to demonstrate that Sandberg recognises its obligations to comply with the GDPR in handling personal data where it is necessary for the ongoing operation of the business. All Sandberg staff and vendors are required to comply with Sandberg's data protection processes at all times.

Sandberg is a UK-based Language Service Provider (LSP) providing translation and localisation services to a worldwide client base consisting principally of other LSPs. Sandberg has offices in the UK, Bulgaria and Sweden. Sandberg provides services in a range of language combinations, with a core focus on translations between English and the Nordic languages, and German and French into English.

As such, Sandberg acts as both controller and processor of personal data, including sensitive personal data, in the following main contexts:

- Sandberg processes content for translation containing personal data, including some sensitive personal data of individuals;
- Sandberg controls and processes personal data of its clients' and prospective clients' staff;
- Sandberg controls and processes personal data of its own staff, and those applying for positions at Sandberg;

Sandberg controls and processes personal data of its subcontractors, including freelance translators and the staff of subcontractor LSPs.

Outline

Personal data audits

Sandberg has undertaken personal data audits within all departments and maintains maps of all data stored.

For each process where personal data is handled, the audit captures the following:

- The types of personal data supplied
- The source/supplier of the personal data
- How the personal data will be processed/why it is being captured
- The legal basis on which that personal data is being processed, e.g.
    - with the consent of the data subject
    - as part of a contract with the data subject
    - because there is a legal obligation to process the personal data
    - where there is a legitimate interest to process the personal data

- Where the personal data is stored
- Who can access the personal data
- How long the personal data will be retained
- Where personal data is sent on to a third party
- Why personal data is sent on to a third party
- Whether the personal data can be deleted if the data subject exercises their right to be forgotten

Annual Review

Personal data audits are reviewed annually. Sandberg is committed to maintaining and developing its documentation and policies as a result of any issues identified in the annual audits, and as further processes incorporating the handling of personal data are identified.

Legitimate Interests Assessments

Sandberg has conducted a Legitimate Interests Assessment where legitimate interest is used as the legal basis for processing personal data.

Processing, transfer and storage of personal data

Sandberg ensures that its staff, subcontractors and third-party processors of personal data handle it securely.

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:

- *Terms & Conditions of Business*
- *Internal Information Security Policy*
- *Vendor Framework Agreement*
- *Vendor Information Security Policy*
- *Internal Vendor Management Process*
- *Internal Recruitment Process*
- *Internal Staff Handbook*

Data retention

Sandberg will ensure that each type of personal data will be retained no longer than its documented data period. Retention periods are documented in Sandberg's data audit documents and relevant policies.

Subject Access Requests

Sandberg will respond to written Subject Access Requests without undue delay, within 1 month, and with no fee chargeable. Sandberg will verify the identity of the requester, and that the request is valid and within the rights of the individual under the requirements of the GDPR.

Requests to be forgotten or Right to erasure

The GDPR provides a right for individuals to have personal data erased. The right is not absolute and only applies in certain circumstances. Sandberg will respond to a verbal or written Request to be forgotten or Right to erasure without undue delay, within 1 month. Sandberg will verify the identity of the requester and their right to request erasure before following internal procedures to delete the relevant data and ensure that any 3rd party processors of the data erase any data Sandberg has shared with them.

Where the legal basis of storing personal data is for contractual or legal obligation, the right to be forgotten is outweighed and in such circumstances, personal data will not be deleted.

Breach notification process

Sandberg will comply with its duty under the GDPR to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. Sandberg will keep a record of any personal data breaches, whether or not legally required to do so.

If a breach is likely to result in a high risk to the rights and freedoms of the affected individuals, Sandberg will inform those concerned directly and without undue delay.

Sandberg will investigate if the breach was a result of human error or a systemic issue and will assess how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

Personal data in content for translation

Sandberg also handles personal data in content for translation, as a sub-processor of that data, sending it on for further processing to freelance translators and LSP suppliers. Sandberg puts great emphasis on handling this data safely and securely at all levels, ensuring personal data in content for translation is handled appropriately throughout the translation process.

A detailed description of Sandberg ‘s processes on handling content for translation can be found in the relevant internal, client and supplier policies.

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 other related regulations take place, additional and more frequent reviews of the policy will take place.