Sandberg's Vendor Privacy Policy

Document control

Version number:	2.1
Policy owner:	Catriona Burns, Talent Programme Manager
Effective date:	25 May 2018
Last review date:	12 February 2024
Next review by date:	12 February 2025

Version control

Ver	Date	Changes
2.1	12 Feb 2024	Content revised; update to the guidance for sharing data with clients.
2.0	6 Feb 2023	Content revised; updated to follow a new policy template; new guidelines for when data is shared with clients; data breach guidelines implemented; policy moved to the website.
1.0	25 May 2018	First version.

Purpose

This Vendor Privacy Policy describes how Sandberg Translation Partners protects and makes use of the information you give the company when you register as a supplier and when you use the Sandberg Passport portal, and outlines when we retain your information for the purpose of contracting you for work.

If you have any questions about this policy, please email our vendor management team at vendor.management@stptrans.com.

Scope

This policy applies to:

- all subcontractors and suppliers to Sandberg Translation Partners in all regions.

Outline

Sandberg gathers and uses certain information about you so that we can engage your services to assist us in the provision of services to our customers.

We may also collect information to better understand how you use Passport and present timely, relevant information to you.

We are committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using Passport, you can rest assured that it will only be used in accordance with this privacy policy.

What do we gather?

When registering on our system, we will ask you to provide the following information, which we collect for contractual purposes:

- Name and job title;
- Contact information including postal and email address;
- Information regarding the setup of your business;
- Your qualifications and professional experience, including your CV and copies of your degree certificates;
- Information on your subject areas so that we can match you against our assignments;
- Rate of pay for services;
- Availability so that we know when we can contact you;
- Payment information so that we can settle your invoices.

During our working relationship, we also gather and retain the following types of information:

- Email correspondence between you and our staff;
- Translation quality feedback;
- A record of projects you have worked on.

What do we do with the information we gather?

We require this information to understand your capabilities so that we may offer appropriate assignments to you, and for the following reasons:

- Internal record keeping;

- To understand the services you may be able to offer to us;
- To engage your services;
- To enable you to invoice us for the provision of your services;
- To enable us to pay your invoices for the provision of your services;
- We may use the information to improve our products and services;
- To contact you via email or telephone to discuss assignments;
- To demonstrate to any of Sandberg's existing or potential clients worldwide your suitability for undertaking linguistic work for them, if they request a copy of your CV for this purpose (see below).

If any of Sandberg's existing or potential clients request a copy of your CV, in order to protect our working relationship with you we only send blind CVs from which your name, address, date of birth, contact details and any other personal data have been removed.

We retain most of your information for the duration of our working relationship, and for a period of seven (7) years thereafter for legal and contractual purposes.

Client security requirements

In exceptional cases, a client may request that we provide the name and details of the suppliers working on their content, in order to fulfil their own compliance requirements. In such cases, we will always seek your consent prior to providing any client with this information, as outlined below.

ID fraud is a real concern and threat to the data security of many clients and therefore some request that the identity of those completing projects for them is verified. Some of Sandberg's clients have high security requirements which require personal verification of the individual each time they access their online systems to complete work. This is to protect access to the content and ensure that only those with the rights to access it do so, and that the person performing the work is the trusted and verified individual.

Initial verification processes for some clients may involve, as an example, requesting to meet with the individual online and view a copy of their passport to confirm their identity before the individual is onboarded to their work. Such a request will only be granted when the client makes a written request in advance explaining their requirement, which is assessed and approved by a member of Sandberg's management team. It is not acceptable for a client to make a copy, screenshot or recording of the meeting or identification document.

If such a request from a client concerns you and your personal details, you will be asked first if you agree to this as part of the onboarding process. If you are not willing to verify your identity in this way, you will not be onboarded to the account or able to take on that particular client's work.

Verification processes for accessing projects on a routine basis may involve two-factor authentication in a similar manner to how an individual verifies their identity when accessing their personal banking or other online service, with either OTCs (one-time codes) sent to their email or mobile phone, or push factor notifications sent to their mobile phone via an authentication app. If you are unwilling to share your phone number with our client for this purpose alone, or if you are unwilling or unable to install an app on a smartphone, you will not be onboarded to the account or able to take on that particular client's work.

Before sharing an individual's contact details with a client, Sandberg will seek the following:

1. Permission from the individual in question.

2. Verification that the client adheres to the GDPR when acting as processors of an individual's personal data, meaning that:

- They will not store, process or use the data for any other purpose than that for which permission was granted, and will delete the data as soon as it is no longer required.
- If they need to pass on the details to a third party (such as the end client), they will only transmit the data in a secure manner and they will ensure the third party also acts in the same respect. In such circumstances, Sandberg's client should always inform Sandberg that they will be forwarding the data on to the third party.
- They will not use the contact details to make personal contact with the individual via telephone call, SMS, email or any other means. If you are contacted by a client of Sandberg's via email, phone or any other means, you should not respond and should immediately notify your Sandberg contact.

Security

We will always hold your information securely, accessible to Sandberg's production staff, our managers, finance department and bank or foreign exchange provider only.

To prevent unauthorised disclosure of or access to your information, we have implemented strong physical and electronic security safeguards.

We also follow stringent procedures to ensure that we work with all personal data in line with the General Data Protection Regulation (GDPR).

Data breaches

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.

Sandberg has a stringent protocol to follow in the unlikely event of a data breach, in line with the recommendations of the Information Commissioner's Office (ICO), the UK's independent body set up to uphold information rights.

Handling of data breaches

In the event of a data breach or a suspected data breach that has resulted in the rights and freedoms of the data subject(s) being affected, Sandberg will notify the ICO within 72 hours without delay.

The Sandberg management team will respond to any breach with containment, recovery, assessment, consideration, evaluation and response.

Data Security Reporting to the Data Subject(s)

If the breach is likely to be of a high risk to a data subject(s), Sandberg will notify the data subject(s) without delay in a clear and concise manner and in accordance with ICO guidance.

We will take the necessary steps to ensure that the high risk that has affected the rights and freedoms of the data subject(s) will no longer affect them.

Sandberg will detail all information relating to the breach of personal data and any facts, communications or reports that result from the breach along with all the actions that have been taken and the effects of the actions.

All users of information, whether internal or external to Sandberg, are responsible for safeguarding data and reporting any actual, suspected or threatened breaches of data, and for assisting in investigations when and as required.

Cookies and how we use them

What is a cookie?

A cookie is a small file placed on your computer's hard drive. It enables our website to identify your computer as you view different pages on our website.

Cookies allow websites and applications to store your preferences to present content, options or functions that are specific to you. They also enable websites to see information such as how many people use the website and what pages they tend to visit.

How we use cookies

The Sandberg Passport website uses a single cookie to identify that a user has logged into the system, and can freely pass between pages without having to reauthenticate their access to the system for the duration that the browser session remains open.

Without this cookie, it would be necessary for the user to log in to every page on the browser.

Controlling cookies

You can use your web browser's cookie settings to determine how our website uses cookies. If you no longer want our website to store cookies on your computer or device, you should set your web browser to refuse cookies.

However, please note that doing this may affect how our website functions. Some pages and services may become unavailable to you.

To learn more about cookies and how they are used, please refer to the Wikipedia article on HTTP cookies.

Controlling your personal information

When you fill in a form or provide your details on our website, you will see one or more tick boxes allowing you to:

- Opt in to receive marketing communications from us by email;
- Opt in to receive request-related notifications from us by email.

Some types of email notifications are mandatory as they are required in order to allow us to carry out our business.

If you have previously agreed to us using your personal information for providing translation services to us, you may change your mind at any time easily, via one of these methods:

- Sign into our website and change your subscription settings;
- Send an email to our vendor management team at vendor.management@stptrans.com.

We will not sell, distribute or lease your personal information to third parties unless we are required by law to do so.

You may request details of personal information we hold on you under the GDPR. If you would like a copy of the information held on you, please email our vendor management team at vendor.management@stptrans.com.

If you believe that any information we are holding on you is incorrect or incomplete, please email our vendor management team at vendor.management@stptrans.com as soon as possible. We will promptly correct any information found to be erroneous.

Compliance measurement

Any employee, sub-contractor, or supplier in breach of this policy may be subject to disciplinary procedures and or appropriate sanctions.

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 privacy-related regulations take place, additional and more frequent reviews of the policy will take place. When we update our Vendor Privacy Policy, we will take appropriate measures to inform you, depending on the significance of the changes made. We will obtain your consent to any material changes to the Vendor Privacy Policy if and where this is required by applicable laws and regulations. You can see when this Vendor Privacy Policy was last updated by checking the 'Last Review Date' displayed at the top. If you continue to use the functions on the Sandberg Passport vendor portal, you are deemed to have accepted the updated Vendor Privacy Policy.