Talking Heads GDPR Policy

"***I want to run a healthy, happy Company.***

The most important element of this is the satisfaction of all the team, suppliers and clients.

The general atmosphere is light-hearted; I wish to encourage a culture of openness, friendliness and transparency. I would like to feel that the team can truly speak their mind at Talking Heads.

This approach is to be combined with utter professionalism.

The team members are encouraged to say their opinion, not be afraid to make suggestions and to take responsibility, not only for their own role, but for the general wellbeing of the Company.

If anyone feesl that I am conducting myself in a manner which does not support this, anonymous or named feedback is encouraged.

Our Company Policies are essential to the well-being of all concerned – they contain guidance that is meant to support the team and the team's actions. There are also legal statements which protect both the employee, and the employer."

Eileen
ee@talkingheads.co.uk

Talking Heads aims to carry out the following documentation and tracking procedures:

- Talking Heads will document as many policies as is appropriate.
- Talking Heads will ensure that their technical infrastructure is capable of implementing their policies; storage of such policies is easily accessible to all the team members.
- Talking Heads will ensure that they have all the resources necessary to implement policies.
- Talking Heads will implement systematic checking procedures to ensure policies are being implemented.
- Talking Heads observes the commission for racial equality's code of practice for employments.

Talking Heads' GDPR Policy

Talking Heads is a data controller. This means we have a valid lawful basis on which to process the personal data (predominantly) of suppliers and (some) customers, as part of our day to day business.
The GDPR applies to our data processing actions as we process data of individuals within the EU. As a course of best practice, we also apply the GDPR guidance to all of our worldwide suppliers' information.

WHAT INFORMATION DOES THE GDPR APPLY TO?

PERSONAL DATA
The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

SENSITIVE PERSONAL DATA
The GDPR refers to sensitive personal data as "special categories of personal data" (Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (Article 10).
Source: ico.org.uk/for-organisations... *Accessed 12-4-2018.*

Article 5 of the GDPR requires that personal data shall be:
"*a) processed lawfully, fairly and in a transparent manner in relation to individuals;*
This policy explains how we process data lawfully and fairly. For reasons of transparency, all processes can be viewed on request.
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
Talking Heads collects the following data from suppliers:

- Qualifications, Experience
- Email address
- Primary Language Pair (Mother Tongue)
- Other languages
- UK bank details (to make payment)
- Certified / Sworn Translator info
- Skype Email
- PayPal Email
- Transport Mode
- Telephone number/s
- CV
- Working Status
- DBS Check
- Memberships
- Previous Clients & Projects
- Employment Status
- CTC Check
- Skrill email
- First Name and Surname
- Address
- Security References
- Software
- Website
- Passport / visa proof to work
- DPSI
- Gender (should a customer require a gender specific linguist)
- Facebook/twitter/instagram
- Proof of address (bill/bank statements)
- Specialism/s
- Photo (for identification during interpreting assignments)
- NINO
- Pastimes (for specialist work)
- Company Name
- Country of Origin
- UTR Number

Talking Heads collects this data for the following reasons:

- To verify identity and right to work status in the UK
- To verify qualifications and professional experience to ascertain suitability to work on specific projects with such demands
- To remunerate suppliers for work undertaken
- To ascertain permission from the supplier about their marketing communication preferences

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Talking Heads will only collect and store data that is absolutely required for the purposes above.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Talking Heads will update any information as soon as possible after we become aware that it is incorrect. Suppliers are provided with an online (password protected) area to keep their information up to date.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

Data which has not been accessed after a period of time may be archived by Talking Heads. This data may be deleted after a period of time.

Under the 'right to erasure' / 'the right to be forgotten' guidance, an individual can request that their data is deleted permanently. There are conditions associated to this which can be found on the ICO website (www.ico.org.uk). An individual who wishes to make this request can email info@talkingheads.co.uk or call 0114 4701075.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Talking Heads will ensure the secure upkeep of data, including but not limited to; conscientious password protection and upholding and up to date deletion of inactive / un-required data.

Article 5(2) requires that: *"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."*

TALKING HEADS RECEIVES AND STORES THE COLLECTED DATA IN THE FOLLOWING WAY:

ONLINE

- Data is collected via online forms which are protected by HTTPS security.
- Some forms we use to collect data are designed by our IT team, who have all signed our Data Protection / GDPR Agreement.
- Some forms we use to collect data are designed on and provided by JotForm (www.jotform.com). Any data collected by JotForm is stored on JotForm's servers, which conform to the EU guidelines (https://www.jotform.com/eu-safe-forms/).

POST

- Usually delivered by the Royal Mail or courier.

PHONE/SMS

- Data collected over the telephone is processed and recorded by our VOIP provider, YayYay Limited t/a yay.com (yay.com/blog/voip-provider/gdpr-compliance/).
- Data collected over the telephone whilst on a conference call is processed by our conference call provider, Via-Vox Limited t/a Powwownow (powwownow.co.uk/privacy).

- Data collected via mobile telephones is processed and stored by our provider, giffgaff (giffgaff.com/boiler-plate/privacy).

EMAIL

- All data is then retrieved (often via email) by our server and saved on our server, which is covered by the following security:
    - All information stored on local servers can only be accessed internally or via encrypted VPN technology.
    - Documents are stored on Windows servers which are fully patched in line with current Microsoft best practice.
    - Access to files is limited by username and password.

OVERVIEW

What personal data do we hold?

Suppliers' personal data as listed above.

Where did it come from?

Primarily provided by suppliers. Sometimes personal information is provided by third-party suppliers such as proz.com.

Who do we share it with?

In the case of standard (written) translation, transcription, typesetting work, etc., we do not share any personal data with anyone outside of our office and team.

In the case of 'Certified' Translation, where we provide a Certificate of Authentic Translation, we provide a certificate showing the suppliers first name, surname, language and sometimes, their qualifications.

In the case of (verbal) interpreting, we share the suppliers first and last name, photograph and language for which the supplier is providing the service on the timesheet supplied for the assignment and the confirmation email. On occasion, customers will request the personal email address and / or telephone number of a supplier. This information will only be given after permission has been granted by the supplier.

TEAM GUIDELINES

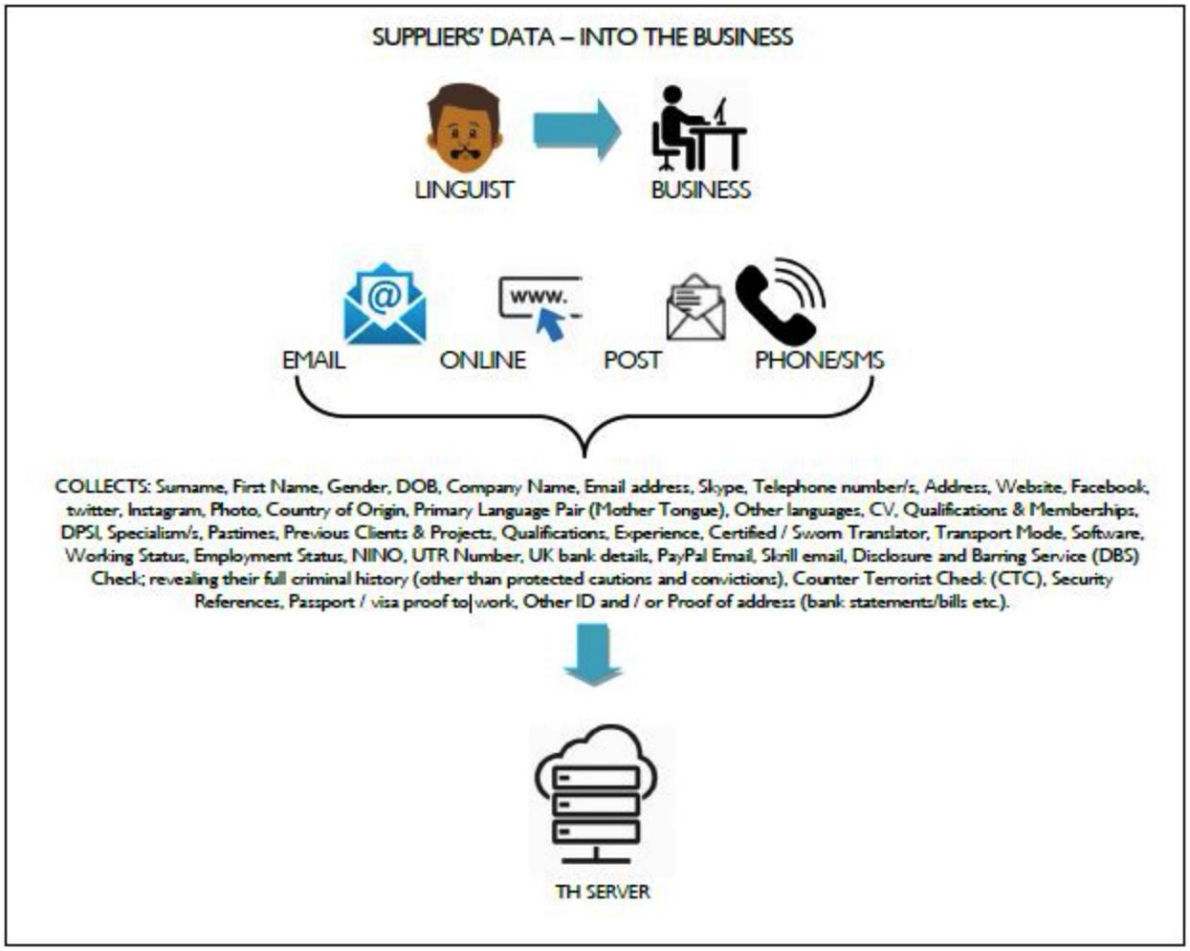
These guideline apply to all employees, freelance workers and contractors who enter the TH office and / or work on TH projects.

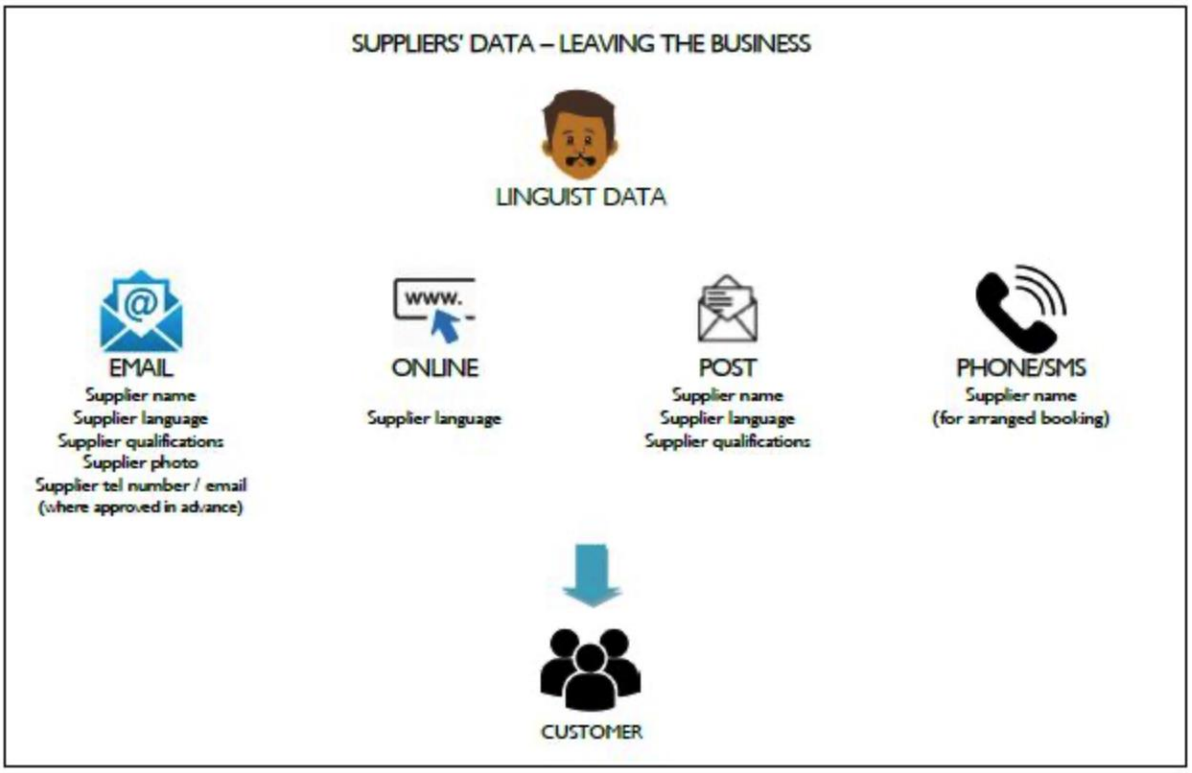
It is your responsibility to ensure that the data you have access to is protected. Actions may include:

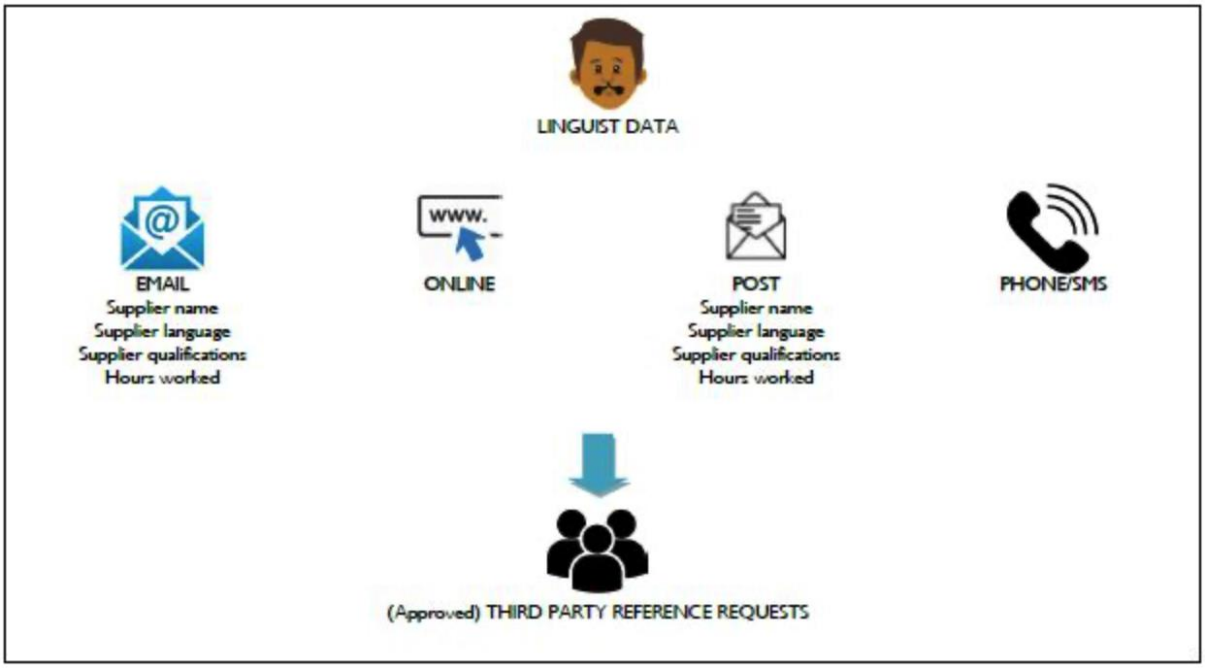
- Not allowing non-authorised persons to have access to / know any identifying / personal data that the company has collected.
- Not informing any outside persons of the company processes or systems or systems providers, such as Jotform etc.
- Do not leave your computer unlocked when you are not in front of it and can protect the data yourself.
- When working remotely, not allowing any non-authorised person to see sensitive data, for example, by looking over your shoulder or by leaving your computer unlocked.

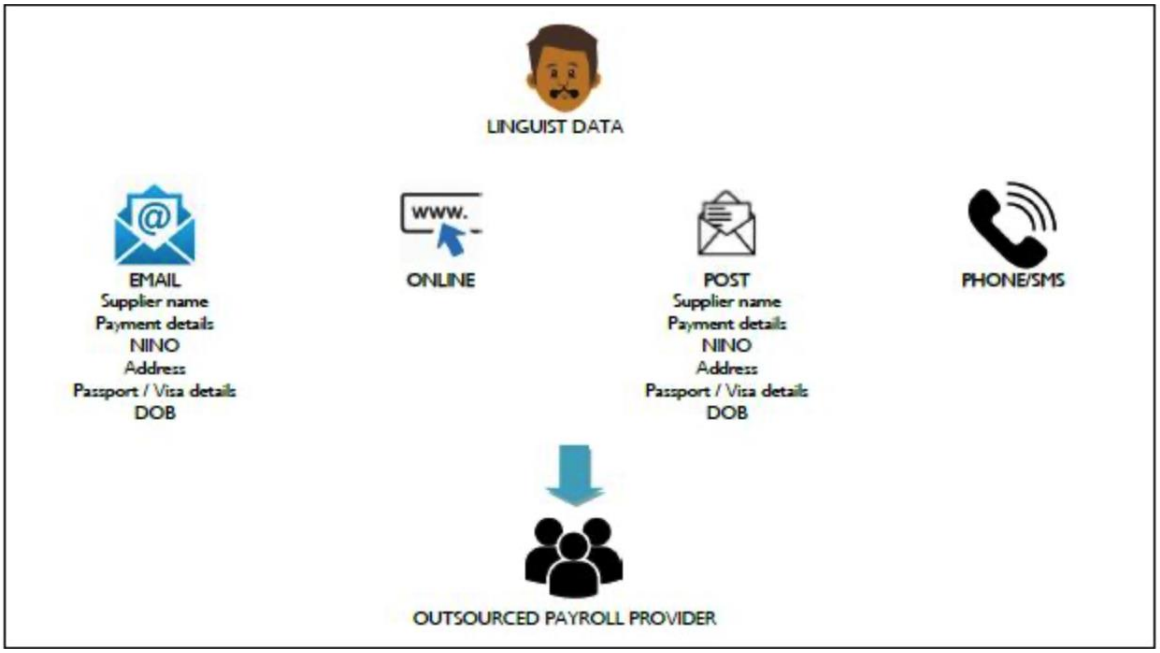
If you have any queries whatsoever, contact your Line Manager or a Company Director immediately.

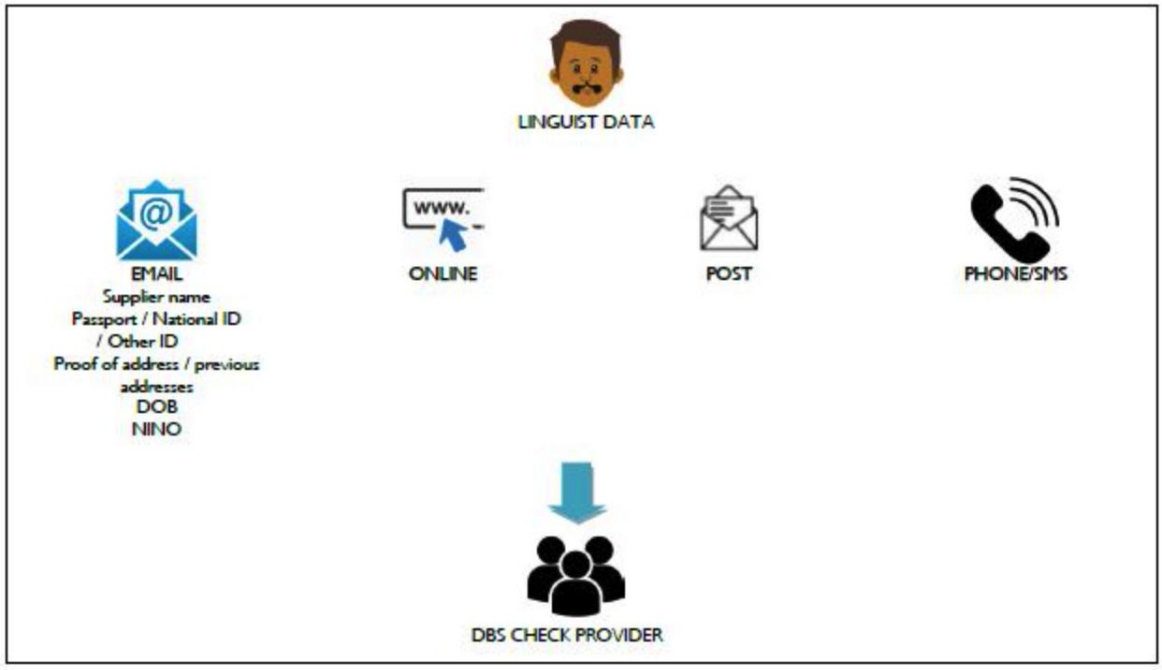
DATA MAPS


SUPPLIERS' DATA – INTO THE BUSINESS
LINGUIST
BUSINESS
EMAIL
ONLINE
POST
PHONE/SMS
COLLECTS: Surname, First Name, Gender, DOB, Company Name, Email address, Skype, Telephone number/s, Address, Website, Facebook, twitter, Instagram, Photo, Country of Origin, Primary Language Pair (Mother Tongue), Other languages, CV, Qualifications & Memberships, DPSI, Specialism/s, Pastimes, Previous Clients & Projects, Qualifications, Experience, Certified / Sworn Translator, Transport Mode, Software, Working Status, Employment Status, NINO, UTR Number, UK bank details, PayPal Email, Skrill email, Disclosure and Barring Service (DBS) Check; revealing their full criminal history (other than protected cautions and convictions), Counter Terrorist Check (CTC), Security References, Passport / visa proof to work, Other ID and / or Proof of address (bank statements/bills etc.).
TH SERVER


SUPPLIERS' DATA – LEAVING THE BUSINESS
LINGUIST DATA
EMAIL
Supplier name
Supplier language
Supplier qualifications
Supplier photo
Supplier tel number / email
(where approved in advance)
ONLINE
Supplier language
POST
Supplier name
Supplier language
Supplier qualifications
PHONE/SMS
Supplier name
(for arranged booking)
CUSTOMER

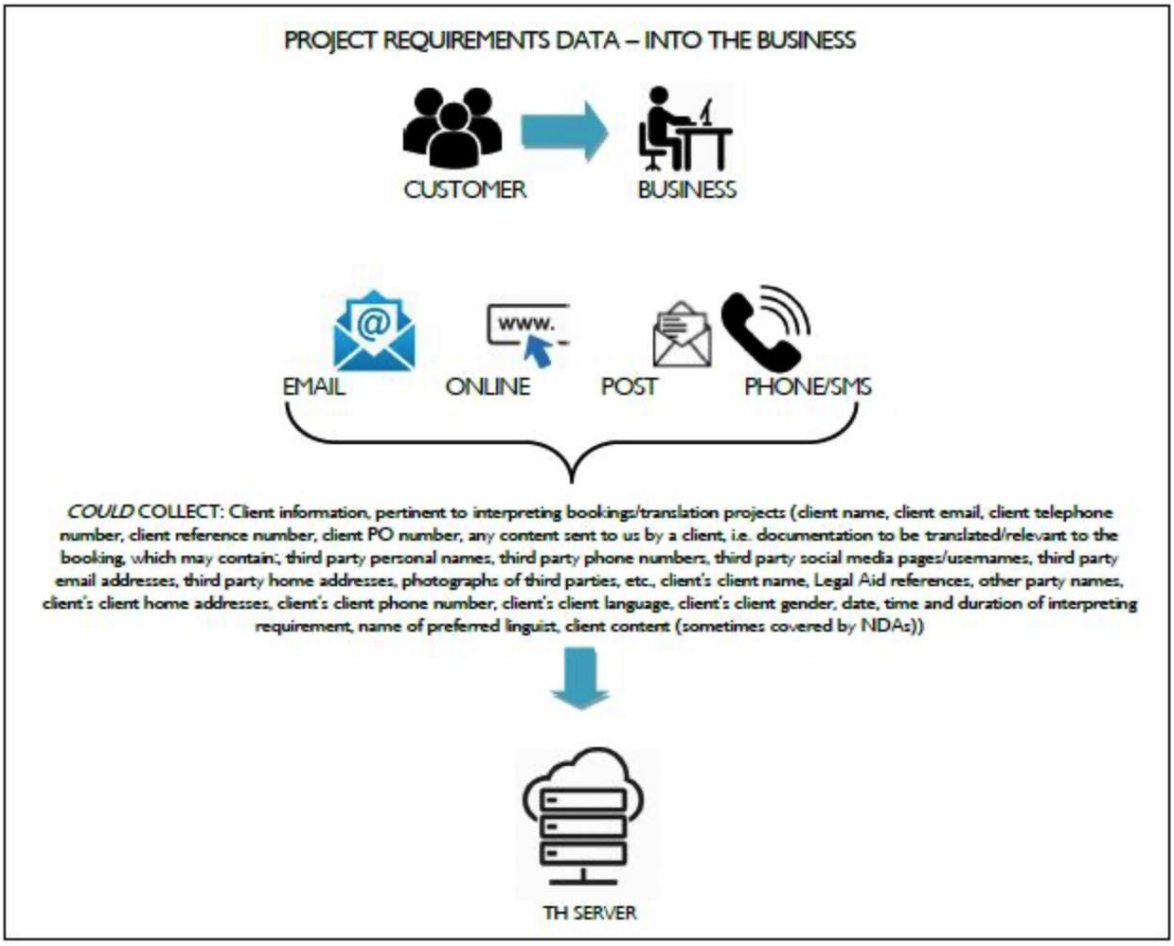

LINGUIST DATA
EMAIL
Supplier name
Supplier language
Supplier qualifications
Hours worked
ONLINE
POST
Supplier name
Supplier language
Supplier qualifications
Hours worked
PHONE/SMS
(Approved) THIRD PARTY REFERENCE REQUESTS

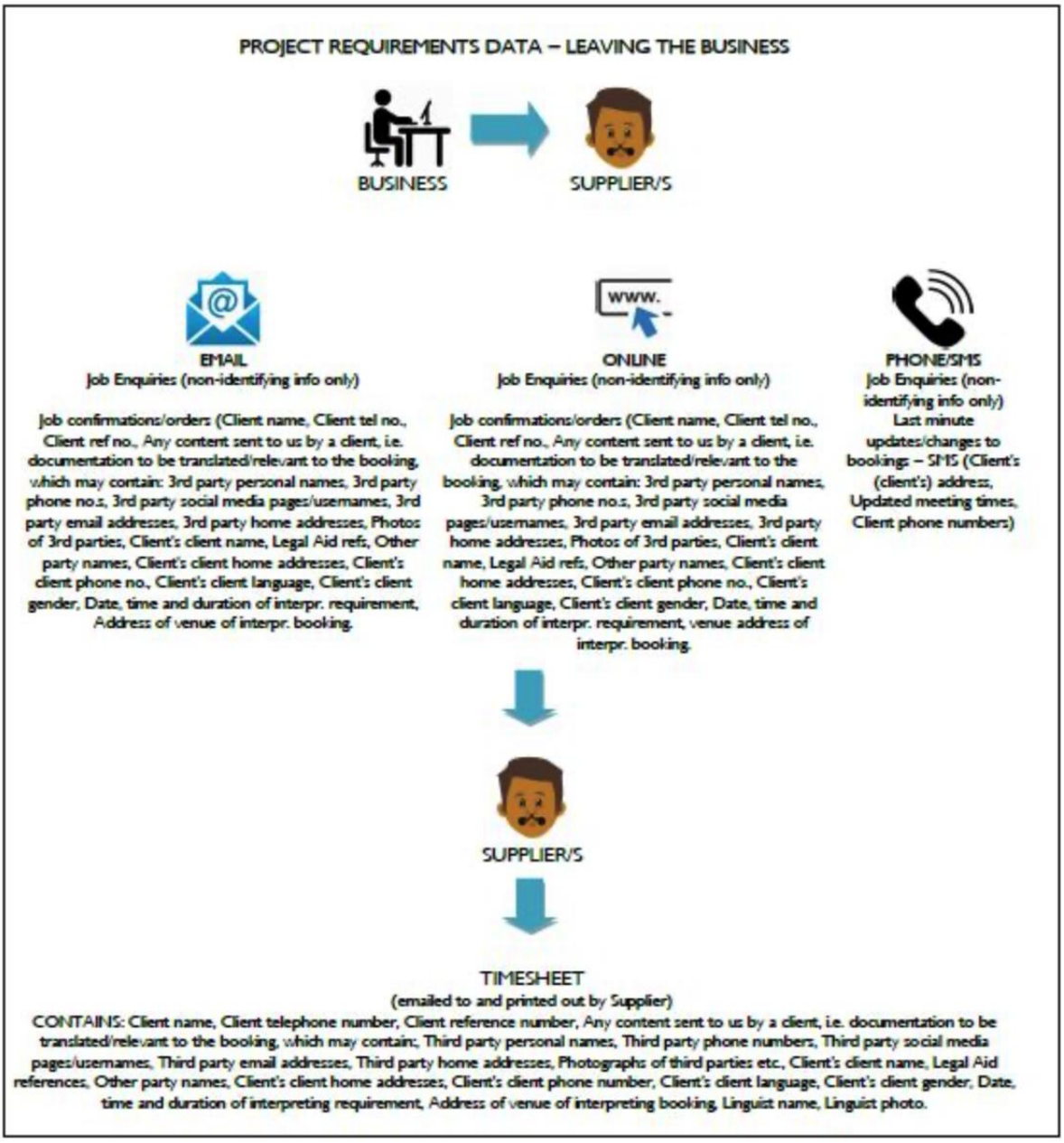




Other

- Remote working: All of the above accessible to TH staff members working remotely, using TH laptops or their own person laptops.
- Internal paperwork: Interpreting diary (Linguist name)
- Data requested by legal authorities for the purpose of carrying out work.


PROJECT REQUIREMENTS DATA – INTO THE BUSINESS
CUSTOMER
BUSINESS
EMAIL
ONLINE
POST
PHONE/SMS
COULD COLLECT: Client information, pertinent to interpreting bookings/translation projects (client name, client email, client telephone number, client reference number, client PO number, any content sent to us by a client, i.e. documentation to be translated/relevant to the booking, which may contain:, third party personal names, third party phone numbers, third party social media pages/usernames, third party email addresses, third party home addresses, photographs of third parties, etc., client's client name, Legal Aid references, other party names, client's client home addresses, client's client phone number, client's client language, client's client gender, date, time and duration of interpreting requirement, name of preferred linguist, client content (sometimes covered by NDAs))
TH SERVER



GDPR CONTACT
Eileen Enos, Director