

## Case Study: How to Ensure GDPR Compliance When Undertaking a Translation Project

By Monique Longton

March 2018

**Please note:** *This document is for informational purposes only and must not be construed as legal advice. Both the client and the translator are advised to consult with their lawyers and legal advisers before they undertake a translation project that falls under the GDPR.*

### Introduction

The [General Data Protection Regulation](#) (the “Regulation” or “GDPR”) will be enforceable as of May 25, 2018. The Regulation aims to strengthen the rights of European Union residents with regard to their personal data. The Regulation defines personal data as “any information relating to an identified or identifiable natural person [...]; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Article 4 of the Regulation). The Regulation confers the following rights to European residents with regard to their personal data:

- Right of access to data
- Right to data portability (right to transmit data to another provider/vendor)
- Right to rectification of data
- Right to be forgotten (erasure of personal data)
- Right not to be subject to a decision based solely on automated processing
- Right to object to certain processing activities
- Protection of minors under 16 years of age
- The option of contacting a supervisory authority in their EU country of residence in the event of a personal data breach

The purpose of this case study is to provide an approach to managing all translation projects that fall within the scope of the Regulation. It is not intended to list all of the obligations that are imposed on *data controllers* and *processors* (as defined in the GDPR). That information can be found in the [Regulation](#). Rather, this document aims to:

- Establish which translation projects must comply with the GDPR
- Provide a procedure for managing a translation project in accordance with the Regulation
- Summarize the client’s and the translator’s obligations at each step of a translation project and make use of the resources made available by the French supervisory authority, the *Commission Nationale de l’Informatique et des Libertés* (CNIL)
- Give an overview of the mandatory terms of the service agreement between the client and the translator when the service agreement is used as an “appropriate safeguard” to govern the relationship between a client and a translator

This document is based on the [Guide for Processors](#) published by the CNIL and on the [Regulation](#). Both the client and the translator are strongly advised to read the Regulation since failure to comply with it can result in heavy fines.

## Which Translation Projects Fall Within the Scope of the GDPR?

To determine whether a translation project involves the processing of personal data covered by the Regulation, we must look at the content of the file to translate. Does it contain personal data of natural persons living in a European Union Member State? If the answer is “yes,” the Regulation is applicable regardless of where the client or the translator is based. The answer to this question is not always obvious. For example, sometimes the client has a document translated because they do not know the language. In such a case, it is best to exercise caution and take all required security measures when sending the document to the translator.

Please also note the Regulation is marked as a “text with EEA relevance.” You should therefore check the [EFTA’s website](#) for the progress of its integration into the EEA Agreement by Iceland, Liechtenstein and Norway.

Examples of documents that might fall within the scope of the GDPR include:

- Employee evaluations
- Civil status records (birth certificate, marriage certificate, etc.)
- Medical records
- Agreements in which a contracting party is a natural person living within the European Union
- Company payroll processing files
- Legal records disclosing the identity of natural persons

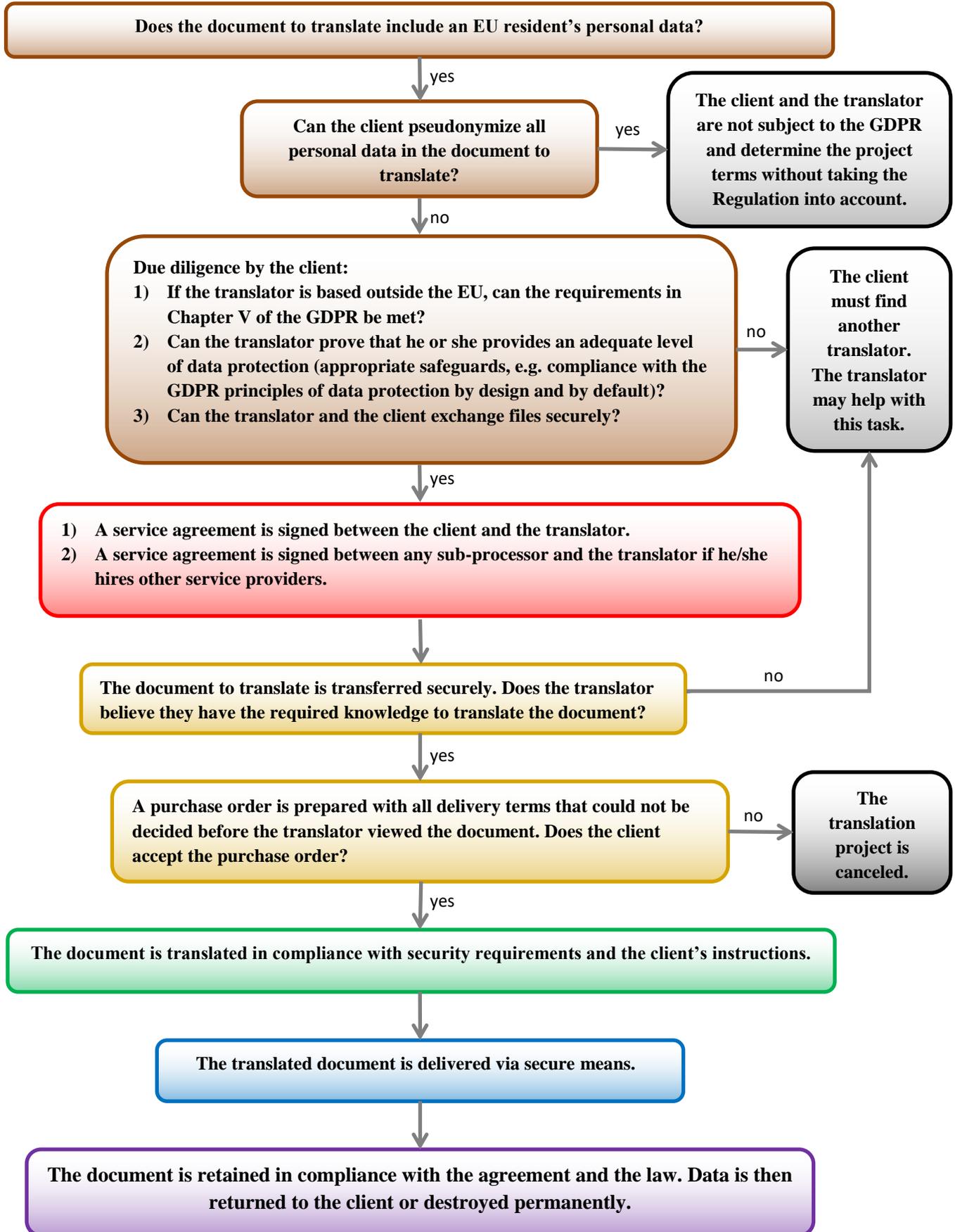
These documents would fall under the GDPR if the persons mentioned in the document are natural persons living within the European Union and the document makes it possible to identify them.

When a translation project falls within the scope of the GDPR:

- The **client**, i.e. the individual or entity who orders the translation services and sub-contracts a translation project to a translator, instructs the translator to translate the documentation and thus assumes the role of controller under Article 4 of the Regulation
- The **translator** becomes a processor under Article 4 of the Regulation by translating the documentation based on his or her client’s instructions
- If the translator hires a **sub-contractor** (reviewer, other linguist, designer, etc.), the sub-contractor becomes a sub-processor and has the same obligations as the translator

## Implementing a Translation Project

The diagram below provides a set of guidelines for implementing translation projects that involve the processing of personal data under the GDPR. The table in the next section summarizes the client’s and the translator’s respective responsibilities under the Regulation at each step of the translation project. A color code is used to provide an easy cross- reference between both sections.



## Obligations of the Client and the Translator at Each Step of the Translation Project

<b>Before Project Launch</b>	
<b>Client's Obligations</b>	<b>Translator's Obligations</b>
<ol style="list-style-type: none"> <li>1) Determine whether the document to translate includes an EU resident's personal data</li> <li>2) Determine whether processing is lawful under the GDPR (Articles 5 and 6 of the Regulation)</li> <li>3) Evaluate a pseudonymization process to hide all personal data</li> <li>4) If the translator is based in a non-EU country, <a href="#">check whether that country has been determined as ensuring an adequate level of protection by the European Commission</a> or whether another "appropriate safeguard" must be in place<sup>i</sup></li> <li>5) Carry out due diligence on the potential translator to determine whether he or she provides an adequate level of data protection (appropriate safeguards, i.e. compliance with the GDPR principles of data protection by design and by default)</li> <li>6) Agree with the translator on which encryption methods to use to send the file to translate</li> </ol>	<ol style="list-style-type: none"> <li>1) Ask the client whether the document to translate contains an EU resident's personal data</li> <li>2) Obtain confirmation from the client that the translation is lawful and fulfills one of the requirements of Article 6 (1) of the Regulation<sup>ii</sup></li> <li>3) Prove to the client that the translator is compliant with the principles of data protection by design and by default; the translator delivers his or her security plan (ISO/IEC 27001:2013 or NIST) and security policy (and indicates who will have access to the file to translate)</li> <li>4) Evaluate whether the translation project requires sub-contracting (e.g. reviewer, other linguist, designer, etc.) and, if so, in which country, and obtain the client's approval</li> </ol>
<b>Project Launch</b>	
<b>Client and Translator's Shared Obligations</b>	
<ol style="list-style-type: none"> <li>1) Draft a service agreement between the client and the translator that includes their obligations (see section below "Mandatory Clauses in the Service Agreement Between the Client and the Translator") or make sure the translation is governed by another legal act (see Article 28 of the GDPR)</li> <li>2) If the translator is based in a non-EU country and the European Commission has not issued an adequacy decision for that country, put in place an "appropriate safeguard"<sup>iii</sup></li> <li>3) Determine a procedure to follow if, after seeing the file, the translator finds that he or she does not have the knowledge to translate it</li> </ol>	
<b>Translator's Obligation</b>	
Tell the client immediately if the instructions violate the Regulation	
<b>File Transfer to the Translator</b>	
<b>Client's Obligations</b>	<b>Translator's Obligations</b>
<ol style="list-style-type: none"> <li>1) Comply with the principle of data protection by design: give the translator only the data that requires translation</li> <li>2) Transfer the file via secure means (data encryption)</li> </ol>	<ol style="list-style-type: none"> <li>1) Store the file in a secure place</li> <li>2) Confirm if the project will be handled and prepare a purchase order with all delivery terms that could not be decided when the translator had not yet seen the file</li> </ol>
<b>File Translation</b>	
<b>Client's Obligations</b>	<b>Translator's Obligations</b>
Ensure that the translator follows the instructions	Translate the file with the utmost confidentiality and security (physical and logical access controls, backups, traceability, encryption, pseudonymization/anonymization)
<b>Optional: Sub-Processing (Review, Design Work, etc.)</b>	
<b>Translator's Obligations</b>	
<ol style="list-style-type: none"> <li>1) Ensure that sub-contractors undertake the translator's obligations as their own (by signing a new sub-processing agreement stating the sub-contractor's obligations under the Regulation)</li> <li>2) Securely transfer the file to the sub-contractor(s)</li> <li>3) Ensure that all sub-contractors store the file in a safe place</li> </ol>	
<b>Translation Delivery to the Client</b>	
<b>Translator's Obligation</b>	
Transfer the file via secure means (data encryption)	
<b>After Delivery</b>	
<b>Client's Obligation</b>	<b>Translator's Obligations</b>
Retain the translation according to the client's contractual and legal requirements	<ol style="list-style-type: none"> <li>1. Retain the translation according to the translator's contractual and legal requirements</li> <li>2. At the end of the retention period: return the data to the client or destroy the data permanently</li> </ol>

## Other Mandatory Requirements Throughout the Translation Project

### The translator must:

- 1) Support the client if the EU resident identifiable/identified in the file decides to exercise his or her rights under the GDPR
- 2) Support the client to fulfill his or her own obligations
- 3) Provide all evidence that demonstrates the translator's compliance with the GDPR and enables the client to conduct audits
- 4) Assume full responsibility toward the client if the sub-contractor does not fulfill his or her obligations
- 5) Impose a non-disclosure obligation on people who work with the translator
- 6) Notify the client of any data breach (such as a cyberattack or a loss of computers or mobile devices that contain the data)
- 7) Designate a representative in the EU if the translator is not based in the EU unless Article 27 (2) of the Regulation<sup>iii</sup> applies to the translator

### The client must:

- 1) Ensure that the translator complies with the Regulation
- 2) Monitor the translation project, which includes conducting audits and inspections of the translator

### Both the client and the translator must:

- 1) Maintain a register with all GDPR data processing activities (see Article 30 of the Regulation) unless they meet the derogation requirements set out in Article 30 (5) of the Regulation<sup>iv</sup> (see the CNIL's drafted registry templates (in French) at <https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-public.xlsx>)
- 2) Designate a data protection officer in certain cases (see Article 37 of the Regulation):
  - a. if they are a public body or authority
  - b. if their core activities enable them to regularly and systematically monitor individuals on a large scale
  - c. if the information to be translated is sensitive data (see recital 10 of the Regulation) or relates to criminal convictions and offences

## Mandatory Clauses in the Service Agreement Between the Client and the Translator

As per Article 28 of the GDPR, “Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.” With this in mind, this section contains a brief overview of the mandatory clauses in the service agreement between the client and the translator if they choose to draw one up. For your convenience, please see the examples of sub-contracting clauses proposed by the CNIL in the [Guide for Processors](#) until the EU standard contractual clauses are published. The following items are mandatory:

- Translation project description (with clear explanations of the processing, the reasons for processing, the data to process, the categories of persons to which data relates and other data provided by the client to the translator)
- Duration of the agreement
- Translator’s obligations:
  - Process the data solely for the purpose stated by the client
  - Process the data in compliance with written instructions
  - Notify the client if the instructions violate the GDPR or any other applicable legislation
  - Obtain the client’s approval to sub-contract the translation project and notify the client if the translation must be sub-contracted in a non-EU country
  - Inform the client if the sub-contractor changes
  - Ensure that the people authorized to see the translation files:
    - Commit to maintain confidentiality
    - Receive the appropriate personal data protection training
  - Help the client respond to requests from identifiable/identified individuals named in the file to exercise their rights
  - Notify the client of any personal data breach by the agreed deadlines and send the necessary documentation to the client to enable him or her to report the breach where necessary to the competent supervisory authority
  - Help the client comply with his or her GDPR obligations
  - Adopt specific security measures
  - Destroy the data at the end of the translation project and provide written evidence of destruction, or return the data to the client
  - Notify the client of the identity of the translator’s data protection officer if the translator designates one
  - Supply the client with all required documentation to prove that the translator has fulfilled all of his or her obligations and enable the client to conduct audits
- Client’s obligations:
  - State the purposes of the translation and supply written instructions
  - Ensure that the translator complies with his or her obligations
  - Monitor the translation project, which includes conducting audits and inspections at the translator’s site
- The translator and the client’s shared obligations:
  - Ensure that the translation file is kept confidential (the translator is therefore prohibited from using public machine translation tools)
  - Comply with the principles of data protection by design and by default
  - Supply information to identifiable/identified persons stated in the file to translate (client and/or translator’s obligation)
  - Maintain a written register for the translation project unless the derogation stated in Article 30 (5) of the Regulation applies

## Conclusion

Complying with the General Data Protection Regulation when undertaking a translation project can be difficult due to the number of participants in the translation cycle. Compliance with the Regulation can only be ensured if all sub-contractors comply with it (all translation agency employees and/or all freelance translators and their reviewers, designers, etc.). Regardless of the number of participants, every project subject to the GDPR will require good communication between the client and their translator. Successful delivery will truly be a team effort where every participant has a role to play.

The GDPR is and will be a continuously evolving topic (e.g. adequacy decision concerning the EU-US Privacy Shield). Readers are therefore encouraged to deepen their knowledge of the Regulation. For further reading, please consider the [websites of the EU countries' supervisory authorities](#), as well as the Article 29 Working Party's website for [guidelines](#) on the Regulation.

---

<sup>i</sup> Article 46(2) of the Regulation:

“2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- (a) a legally binding and enforceable instrument between public authorities or bodies;
- (b) binding corporate rules in accordance with Article 47;
- (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.”

---

**ii Article 6 (1) of the Regulation:**

“1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”

**iii Article 27 (2) of the Regulation:**

“2. The obligation laid down in paragraph 1 of this Article shall not apply to:

- (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
- (b) a public authority or body.”

**iv Article 30 (5) of the Regulation:**

“5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.”