

#TranslatingEurope  
#TEWGDPR

# Translating Europe Workshop Project Report



## Towards Common European GDPR Guidelines for the Translation and Interpreting Profession

April 2022

### **Authors**

Stefanie Bogaerts, FreeLING Foundation

John O'Shea, FIT Europe

Raisa McNab, EUATC

# Introduction

## Introduction

Data protection is an increasingly important issue for the translation and interpreting (T&I) profession. The General Data Protection Regulation's purpose is to bring order to the data processing arena, but a lack of uniform interpretation of the GDPR across Europe has resulted in discrepancies in working practices, and many grey areas remain around the implementation of the GDPR within the T&I sector.

Translators, interpreters, and language service companies routinely work in cross-border contexts, and it is imperative for the T&I sector to come together to identify issues around the implementation of the GDPR, shine a light on existing grey areas, and proceed to present sector-specific interpretations and conclusions.

To increase the level of GDPR compliance, and to ensure uniform implementation across Europe and internationally, there is an urgent need for specific guidelines for the T&I sector. These guidelines should answer major questions about the procedures and formalities connected with data processing in the sector and propose best practices.

I take heart in the workshop address delivered by European Data Protection Supervisor Wojciech Wiewiórowski. The T&I sector is one of the first in Europe to address the challenges and practical solutions around GDPR implementation in a collective, collaborative fashion, and we have the full support of the EDPS as well as the European Data Protection Board in our endeavours.

It is my great pleasure to present to you the first part of this journey, a report on the results of this Translating Europe Workshop *Towards Common European GDPR Guidelines for the Translation and Interpreting Profession*, carried out as a pan-European collaboration of the European Commission Directorate-General for Translation, FIT Europe, the FreeLING Foundation, and other partners.

**Krzysztof Nalepa**

Field Officer, Warsaw Field Office

European Commission Directorate-General for Translation

# Project summary

## Project summary

The General Data Protection Regulation (GDPR) came into force in 2018, but the T&I sector in particular has suffered from a lack of consistent application and implementation of the GDPR, resulting from grey areas around compliance, and inconsistent guidance from national data protection authorities.

In the T&I sector, the presence of personal data in translated and interpreted content poses unique challenges. Personal data in this type of content is not structured, but ad hoc, almost incidental, and as such challenging to process in a consistent, safe manner. What is more, clients are often unaware or ignorant of their obligations towards safe processing of personal data in the content they send for translation or interpreted content.

This Translating Europe Workshop is the first step towards common European GDPR guidelines for the translation and interpreting profession. It encompasses the work of a panel of legal and T&I sector experts, an all-day online workshop with T&I professionals, and this summary report.

The report outlines key challenges in the implementation and compliance of the GDPR in the translation and interpreting profession, explored and analysed by the pan-European panel of experts.

The report explores six specific areas of interest:

- Types of personal data handled in the T&I sector
- Language Service Providers' roles as data controllers and processors
- Contractual agreements between controllers and processors
- The use of sub-processors in the T&I sector
- Issues and solutions around data retention
- Identifying, analysing, and mitigating risks

Each area is presented in summary form with the expert panel's key findings, followed by a more detailed analysis. At the end of the report, we present the expert panel's conclusions and a proposal to continue this important work and to create practical, T&I sector specific guidelines.

This TEW GDPR project encompasses both individual translators and interpreters working as freelancers, and language service companies. GDPR applies to all, and within this project, we use the term Language Service Provider (LSP) to refer to any natural or legal person providing T&I services. From a GDPR perspective, there can be no distinction between freelance professionals and language service companies. The only difference lies in their role within the T&I supply chain.

Tackling the T&I sector's challenges, our work has brought clarity on many of the main issues, for example, around LSP roles and contractual requirements. We have come to consistent interpretations and present here a position on the major issues concerning data protection and processing in the T&I sector.

The findings of the expert panel, while well-considered and justified, do not however constitute legal advice, and every LSP is advised to ensure that their unique activities comply with the GDPR's specific requirements.

While we have been able to shine a light on existing grey areas, further work is needed to establish valid interpretations of the GDPR's requirements.

This project has also revealed a real need for practical, T&I sector specific guidance on applying and implementing GDPR. We propose to continue this work through another Translating Europe Workshop in 2023, focusing on creating that guidance, and raising the level of GDPR awareness and compliance across the T&I sector and among their clients.

At the heart of the GDPR is the principle of protecting individuals' personal data, and this we must do throughout the often complex T&I supply chain, from the data controller to the LSP processor and their sub-processors, and back again.

**Stefanie Bogaerts**

TEW GDPR Project Leader

President of the Board, FreeLING Foundation

**John O'Shea**

TEW GDPR Project Leader

Chairperson, FIT Europe

# Table of contents

## Table of Contents

Introduction.....	2
Project summary .....	3
Types of personal data summary .....	7
Types of personal data analysis.....	8
Processing data in translated content .....	9
Processing data in interpreted content .....	9
LSP as controller and processor summary .....	11
LSP as controller and processor analysis.....	12
LSP as controller of client data .....	14
Considerations around judicial authorities .....	15
Considerations around natural persons as clients .....	16
A processor’s obligations .....	17
Contractual agreements summary.....	19
Contractual agreements analysis .....	20
International data transfers .....	21
Further issues around contractual agreements and obligations of the processor .....	21
Use of sub-processors summary .....	23
Use of sub-processors analysis.....	24
Lists of sub-processors .....	24
Data retention.....	26
Data retention summary .....	26
Data retention.....	27
Data retention analysis.....	27

Retention of translated or interpreted content.....	27
Establishing data retention periods .....	28
Data retention in translation memories .....	28
Data anonymisation .....	29
Risk mitigation.....	30
Conclusions and next steps .....	31
Project partners.....	32
Project experts .....	33
References.....	36

# Types of personal data

## Types of personal data summary

LSPs routinely process two types of personal data: administrative data, and data in translated or interpreted content.

Administrative data includes client, supplier, and employee data. These data are not specific for the T&I sector, and in handling these kinds of data, LSPs' business activities are comparable to any other sector.

Handling personal data in translated or interpreted content is very specific to the T&I sector. The challenges around processing personal data in translated or interpreted content focus around the ad hoc, incidental nature of such data, the technical challenges of managing the data, and T&I clients' and supply chain's awareness of their obligations under the GDPR.

## TEW expert panel's conclusions

The TEW expert panel has encountered diverging views on whether the GDPR applies to the handling of personal data in translated or interpreted content.

In the TEW expert panel's view, **translation of content containing personal data is processing of personal data** as outlined in the GDPR, if it is done by automated means, or if the output is integrated or intended to be integrated in a filing system. This is the case for the vast majority of translation activities.

**There is no doubt that LSPs carry out processing activities of personal data in translated content, and the GDPR applies to the processing of these data.**

However, the TEW expert panel's opinion is that **interpreting should not be considered as processing under the GDPR**, unless automated support is used, or the interpreting is recorded.

**If interpreting is supported by automated means, or recorded, interpreting services can be considered as data processing, and as such come under the GDPR.**

## Resources

[European Data Protection Board \(EDPB\) Guidelines on the concepts of controller and processor in the GDPR](#)

# Types of personal data

## Types of personal data analysis

There are two types of personal data LSPs routinely process: administrative data, and data in translated or interpreted content.

ADMINISTRATIVE DATA	TRANSLATED/INTERPRETED DATA
<p>Administrative <b>client data</b> such as a person's name, address, telephone number, or e-mail</p> <p>Administrative <b>supplier data</b> with a similar scope as client data</p> <p>Administrative <b>employee data</b> such as an employee's name, address, or ID number</p>	<p><b>Personal data</b> contained in translated content</p> <p><b>Personal data</b> contained in interpreted content</p>

Administrative personal data are not specific for the T&I sector, and as such, LSPs are comparable to any other business, in terms of handling personal data in the course of their business activities, and in complying with the GDPR.

Most national data protection authorities have published comprehensive guidelines and templates for managing administrative data, and LSPs are advised to make use of these resources. GDPR compliance and implementation relating to administrative data is outside the scope of this TEW project and report.

Handling personal data in translated and interpreted content, on the other hand, is very specific to the T&I sector, and issues around GDPR compliance and implementation around these data are discussed in detail in the chapters of this report.

Personal data in translated or interpreted content can often be classified as normal personal data with a low risk, for example, the name and contact details of a company's employee that are also freely available on the company's website. However, it can also be sensitive personal data with a high risk associated with it, for example, information frequently encountered in medical translations such as an individual's medical report.

Article 9 of the GDPR defines sensitive personal data as follows:

*[...] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation [...].*

A high risk can also be attached to sensitive personal data encountered in legal translation and



sworn/state-authorized translations, such as criminal records, defined as criminal data in Article 10 of the GDPR:

*[...] personal data relating to criminal convictions and offences or related security measures [...]*

### ***Processing data in translated content***

Within the T&I sector, there are diverging views on whether the GDPR applies to the handling of personal data in translated content.

The TEW expert panel has encountered the opinion that, as the processing of data in translation activities is purely incidental, and not the goal of translation services, the GDPR should not apply to this activity. Such a view has – at some point – been expressed, for example, by the German Bayern Data Protection Authority, Bayerisches Landesamt für Datenschutzaufsicht<sup>1</sup>.

The TEW expert panel refutes this interpretation, and asserts that, in general, translation of content containing personal data is *processing of personal data* as detailed in the GDPR, if it is done by automated means, or if the output is integrated or intended to be integrated in a filing system. This is the case for the vast majority of translation activities.

Although personal data in translated content are incidental, and have no meaning or use for the translator *per se*, they are the personal data of a natural person, the data subject, and should therefore be appropriately and adequately protected.

This view is also indicated in Paragraph 44 of the European Data Protection Board’s Guidelines:

*Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a “controller” even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data.*

In the TEW expert panel’s opinion, there is no doubt that LSPs carry out processing activities of personal data contained in content for translation. As such, all the relevant provisions of the GDPR apply to the processing of these data.

### ***Processing data in interpreted content***

Spoken and non-spoken interpreting has, so far, been an underexplored area of GDPR compliance. The TEW expert panel analysed whether interpreting oral or signed communication containing personal data should be defined as data processing.

To approach this question, we first turn to the definition of ‘processing’ in Article 4 of the GDPR:

*[processing is defined as] any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or*

---

<sup>1</sup> [https://www.lida.bayern.de/media/FAQ\\_Abgrenzung\\_Auftragsverarbeitung.pdf](https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf)

*combination, restriction, erasure or destruction.*

Can interpreting be defined as ‘adaptation or alteration’, ‘dissemination’, or ‘making available’ of personal data? In the opinion of the TEW expert panel, this processing activity is not sufficient to define interpreting as personal data processing.

However, returning to the material scope of the GDPR, defined in Article 2, interpreting can be considered as data processing if the oral or signed communication is

- processed wholly or partly by automated means, i.e., the interpreting itself is supported by technical infrastructure, for example, carried out using a commercial interpreting platform; or
- if the interpreting is recorded and stored and leaves a permanent trace in a filing system.

The TEW expert panel therefore sees that interpreting, that is, human transfer of speech or signing from one language into speech or signing in another language, should not be considered as processing under the GDPR.

However, if any automated support is used, or the interpreting is recorded in any way, interpreting services can be considered as data processing, and as such come under the provisions of the GDPR.

# LSP as controller and processor

## LSP as controller and processor summary

The concepts of data controller and data processor play a crucial role in the implementation of the GDPR in the T&I sector, as they determine who is responsible for compliance.

A data controller determines the purposes and means of the processing of personal data. A data processor processes personal data on behalf of the controller, under the controller's instructions.

## TEW expert panel's conclusions

LSPs are data controllers for client, supplier, and employee data, like any other business.

In the TEW expert panel's view, when it comes to data in translated or interpreted content, **LSPs are data processors for processing personal data in content received from a client, when the data are processed under the client's instructions.**

However, LSPs also routinely retain and use client content in data repositories such as folder structures and translation memories, and often these data are retained indefinitely.

**A key finding of the TEW expert panel is that further processing of client data for an LSP's own purposes, for example, retaining data in translation memories, makes the LSP a data controller of that data, with all of its associated obligations.**

New guidance from the French Data Protection Authority CNIL indicates that such processing *can* be lawful if permission for further processing is granted by the primary controller, and certain requirements are met. The TEW expert panel advises caution for any LSPs using this option.

A further consideration around the role of an LSP is the type of the client. The TEW expert panel has identified a number of challenges around an LSP's authority to process personal data in judicial documents, and calls for further clarity from national data protection authorities in the matter.

With natural persons, clients who are private individuals, in the TEW expert panel's view, the role of the LSP does not change. **A private individual client is a data controller, even if they have a limited ability to act as one. An LSP is a data processor, but has a responsibility to ensure that appropriate contractual agreements and safeguards are put in place with the controller.**

## Resources

[European Data Protection Board \(EDPB\) Guidelines on the concepts of controller and processor in the GDPR](#)

[CNIL guidance on processors processing data for their own purposes](#) (in French)

[International Association of Privacy Professionals' analysis of CNIL guidance](#) (in English)

# LSP as controller and processor

## LSP as controller and processor analysis

One of the key elements around GDPR compliance in the T&I sector is the role of an LSP in the processing of administrative data, on one hand, and translated or interpreted content, on the other. This is where there also exists a considerable lack of clarity within the sector.

The TEW expert panel presents a model for common practices in the T&I sector below, but urges every LSP to review its own situation and assess whether its processing activities fit into the model presented.

Inconsistencies in interpretation start with the basic concepts of data controller and data processor. These concepts play a crucial role in the implementation of the GDPR, as they determine who is responsible for compliance.

The two key roles within the GDPR are those of a data controller and data processor, defined as follows in Article 4:

*Controller: (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (...)*

*Processor: (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*

To define an LSP's role as a controller or processor, we consider who determines the purpose and the means of processing.

Paragraph 26 of the EDPB Guidelines states that

*the need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.*

When it comes to administrative data, client and supplier data is processed in order to identify clients and suppliers, communicate with them, send quotes, accept projects, invoice finished services, send marketing messages, etc. Employee data is processed, for example, for entering into an employment contract or for administrating payroll.

With administrative data, the purpose and means of processing administrative personal data are determined by the LSP. LSPs are data controllers as far as client, supplier and employee data are concerned.

Personal data contained in translated or interpreted content is processed in order to carry out

translation or interpreting services on a client's instructions. The client determines the purpose and essential means of processing.

In the TEW expert panel's view, when it comes to personal data in translated or interpreted content, LSPs are data processors for processing personal data in the content they have received from the client, when the data are processed under the client's instructions.

It is the client who initiates the processing, and decides its purpose, typically, translating content into another language. It is the client who decides for what purpose the translated document will eventually be used, and the essential means of processing.

While the LSP exerts some control over the means of processing, for example, in their choice of technical means to carry out the processing, the TEW expert panel sees these means to be 'non-essential', meaning the client retains the role of the controller.

'Essential means' are those referred to in Article 28(3) of the GDPR, which must be set out in the data processing agreement and include the subject matter, duration, nature and purpose of processing, and the type of data and data subjects.

By contrast, 'non-essential means' refer to the technical means used to process the personal data (such as the choice of software), the details of which are left to the data processor – the professional in the arrangement – to decide, although it is recommended that they be described, at least in general terms, in the agreement between the data controller and the data processor.

The concepts of essential and non-essential means are further explained in Paragraph 40 of the EDPB Guidelines:

*As regards the determination of means, a distinction can be made between essential and non-essential means. "Essential means" are traditionally and inherently reserved to the controller. While nonessential means can also be determined by the processor, essential means are to be determined by the controller. "Essential means" are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?"). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.*

However, the LSP may also process content for translation or interpreting for purposes other than those defined by the client. In such a case, the purpose and means are defined by the LSP. This is a key finding of the TEW expert panel.

LSPs are data controllers for processing personal data in translated or interpreted content if they process the data further for their own purposes.

If the LSP processes personal data in the content received from the client for further purposes, such as feeding translation memories, training machine translation engines, recording interpreting assignments, or improving their quality of services or training, this will make the LSP a controller of

these data.

In summary, we can draw the below table to detail an LSP's roles.

LSP = CONTROLLER	LSP = PROCESSOR
<ul style="list-style-type: none"> <li>• administrative client, supplier and employee data</li> <li>• personal data data in translated/interpreted content processed for the LSP's own purposes, outside of the client's instructions</li> </ul>	<ul style="list-style-type: none"> <li>• personal data contained in content for translation or interpret content, processed according to the client's instructions</li> </ul>

### *LSP as controller of client data*

A key consideration of significant consequence is what happens when an LSP defines its own further purposes for processing personal data in translated or interpreted content, outside of the purposes of the client-controller, and their instructions. Can the LSP lawfully step outside the framework of the data processing agreement?

It is accepted common practice within the T&I sector for LSPs to retain and use client content to feed translation memories, and to retain content in other data repositories including folder structures or machine translation engines. Many LSPs also retain client content indefinitely, for future reuse, or against complaints or liability.

**This type of processing infringes the GDPR, as these purposes are established by the LSP, not by the data controller. As such, the LSP turns into a controller of the data, as detailed in Article 28(10) of the GDPR:**

*10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.*

However, guidance from the French Data Protection Authority CNIL indicates that such processing *can* be lawful if permission for further processing is granted by the primary controller, i.e., the client, and the following requirements are met:

- the original controller grants explicit permission;
- the new purpose is "compatible" with the original purpose for processing; and
- the data subject has been duly informed about the possibility of further processing.

This requires the LSP to clearly specify how and why personal data will be reused and to ensure that the client-controller grants sufficient permissions in the contract. The client-controllers must also evaluate whether their processors' new purposes are compatible with the initial processing

purposes. The client-controller will also have to notify the data subjects and inform them on their ability to object to the processor's further processing.

If granted the right to further process the data for their own purposes, an LSP becomes a controller of the data, with all the associated obligations of a controller.

It should be noted that this approach has not been confirmed by the European Data Protection Board, whose executive summary details that 'a processor must not process the data otherwise than according to the controller's instructions'. Further in Paragraph 81 the EDPB Guidelines state that:

*"Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.*

### ***Considerations around judicial authorities***

A further consideration around the role of an LSP is the type of the client. The GDPR defines controller as a 'natural or legal person, public authority, agency or other body'.

Legal persons, typically, companies or other organisations, pose no great difficulties in terms of GDPR compliance.

However, the TEW expert panel sees a number of challenges and remaining grey areas around public authorities, and judicial authorities in particular.

Diverging national legislation and legal practices make it very difficult to draft guidelines at a European level.

Local national legislation on sworn or state-authorized translations exists in many EU member countries, and in these countries, processing of personal data, for example, on criminal convictions, may be authorised by the national Member State Law. However, other EU member countries have no such legislation, and the authority with which T&I professionals process judicial documents containing personal data can be called to question.

Another remaining grey area in relation to judicial authorities lies in the provisions and application of the Law Enforcement Directive (Directive (EU) 2016/680), which contains rules on data protection very similar to those in the GDPR.

The TEW expert panel calls for further clarity, and guidance from national data protection authorities in each Member State, to ensure that the requirements for fulfilling the conditions of Article 10 of the GDPR are understood across the T&I sector, specifically with regards to the definition of 'appropriate safeguards':

*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. (...).*

### *Considerations around natural persons as clients*

Natural persons as clients are, within the T&I sector, typically individual people requiring translation of documents into another language for personal purposes.

Paragraph 17 of the EDPB Guidelines indicates that a natural person may act as a controller under the GDPR:

*[...] in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.*

However, the role of an LSP providing translation services to a natural person has proved problematic in the sector, with varied interpretations.

The main challenge around private individuals as clients is that they typically have very limited knowledge of the GDPR and a controller's responsibilities, and a limited ability to apply a controller's obligations.

The TEW expert panel has encountered views that the GDPR does not apply to the processing of personal data 'by a natural person in the course of a purely personal or household activity' (Art. 2(2)(c)), and that a private person therefore cannot be a controller. As a consequence, it is the LSP who must become the controller of the content for translation or interpreting.

The TEW expert panel refutes this notion. Even if the client is exempt from the GDPR when they are acting in the course of purely personal or household activities, the role of the LSP cannot change.

The TEW expert panel's interpretation is based on Recital (18) of the GDPR:

*(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.*

When processing data for natural persons, the LSP remains a processor, even if the client is not capable of fulfilling, or does not have to fulfil their obligations as a controller. In processing data for natural persons, LSPs perform the same processing activities as when their client is a legal person.

On the controller's and processor's joint responsibility for ensuring contractual agreements are in place, paragraph 101 of the EDPB Guidelines states:

*Since the Regulation establishes a clear obligation to enter into a written contract, where no other relevant legal act is in force, the absence thereof is an infringement of the GDPR. Both the controller and processor are responsible for ensuring that there is a contract or other legal act to govern the processing.*

In practice, when the client is exempted from the GDPR or cannot conceivably carry out the obligations of a controller under the GDPR, some of the obligations and responsibilities of the



controller will be fulfilled the processor in order to safeguard the processed data, and to ensure that the processor is able to comply with their obligations under the GDPR.

Here, the TEW expert panel strongly recommends that the LSP as a processor prepares the contractual agreements to offer to their client, and decides on adequate technical and organisational measures to secure the data.

Because content for translation often contains not just the client's own personal data, but that of third parties, the expert panel further advises that the contract between the client and the LSP should include provisions stating that the personal data in the content for translation was obtained by the client in a lawful manner, and that they are entitled to process it. This is a matter of client education, and a concrete way in which LSPs can help raise awareness of GDPR among society.

The TEW expert panel recommends that all crucial decisions, typically taken by the controller, should be outlined explicitly in the contractual agreements signed by the client.

### *A processor's obligations*

As a processor of client data, an LSP is subject to a number of obligations built around the concept of helping the data controller to meet its obligations under the GDPR. These are briefly outlined below.

As a processor, an LSP is obliged to fulfil its obligations specified in Articles 28, 30, 31–33 and 37 of the GDPR:

- **process** the personal data only **on documented instructions from the controller**, unless required to do so by Union or Member State law to which the processor is subject;
- implement appropriate **technical and organisational measures to ensure a level of security** appropriate to the risk and assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the processor;
- maintain a **record of** all categories of **processing activities** carried out on behalf of a controller;
- cooperate, on request, with the supervisory authority in the performance of its tasks;
- ensure that persons authorised by the LSP to process the personal data have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality;
- **not engage another processor without prior specific or general written authorisation** of the controller;
- taking into account the nature of the processing, **assist the controller** by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR;

- at the choice of the controller, **delete or return all the personal data to the controller after the end of the provision of services** relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data;
- make available to the controller all information necessary to **demonstrate compliance** with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;
- **notify** the controller without undue delay after becoming aware **of a personal data breach**; and
- **designate a data protection officer** in cases specified in Article 37 GDPR.

# Contractual agreements

## Contractual agreements summary

A contractual agreement between a controller and a processor 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. The contract should also stipulate the obligations of the processor. Any transfers of personal data to a third country, a routine activity specific to the T&I sector, must also be contractually agreed between the client-controller and their processor.

The GDPR does not require a contract to be in a specific format. In practice, a Data Processing Agreement (DPA) may be self-standing, or incorporated in the contract between the client and the LSP. Controllers and processors may also make use of Standard Contractual Clauses (SCCs), which include model agreements that can be used 'as is', in lieu of a free-form Data Processing Agreement.

## TEW expert panel's conclusions

The TEW expert panel acknowledges that T&I clients' lack of awareness of their obligations as controllers under the GDPR is a significant issue in the T&I sector. **It is the controller's and the processor's shared responsibility to ensure that appropriate contractual agreements are in place, and that the agreed provisions are also implemented in the contractual agreements with the LSP's suppliers, service providers and subcontractors.**

In the TEW expert panel's view, where a client is unaware of or ignores their obligations, the LSP should take a proactive approach to ensure GDPR compliance. This may often mean providing the client with a Data Protection Agreement or appropriately prepared SCCs.

**The TEW expert panel recommends the use of SCCs without modification as the safest practice to ensure GDPR compliance,** with the SCC annexes appropriately filled in.

The TEW expert panel recognises that grey areas remain in the scope of transfers to third countries, and calls for further expert analysis and guidance around this area.

Due to varied practices and continued uncertainty around contractual agreements within the T&I sector, the TEW expert panel would welcome sector-specific Standard Contractual Clauses as a tool for promoting uniform and consistent standards, and to give LSPs the legal and organisational certainty they seek when entering in contractual agreements with clients and suppliers.

## Resources

[Standard Contractual Clauses between controllers and processors](#)

[Standard Contractual Clauses for the transfer of personal data to third countries](#)

# Contractual agreements

## Contractual agreements analysis

Processing of personal data contained in content for translation or interpreted content should be governed by a contract or other legal act under Union or Member State Law.

The contract 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. The contract should also set out the processor's obligations as specified in Article 28 (3) (a-h) of the GDPR.

Contractual agreements between the controller and the processor should also govern transfers of personal data to a third country, a routine activity specific to the T&I sector.

The GDPR does not require a contract to be in a specific format. In practice, a Data Processing Agreement (DPA) may be self-standing, or incorporate in the contract between the client and the LSP. Controllers and processors may also make use of Standard Contractual Clauses (SCCs), which include model agreements that can be used 'as is', in lieu of a free-form Data Processing Agreement.

Standard Contractual Clauses (SCCs) are a modular mechanism to contractually govern the relationship between a controller and a processor, between the processor and their sub-processors, and the transfer of personal data outside the EU/EEA.

There are two sets of European Commission's SCCs:

- Standard Contractual Clauses between controllers and processors inside the EU/EEA
- Standard Contractual Clauses for the transfer of personal data to third countries

Although the use of the SCCs is not mandatory, the TEW expert panel recommends their use without modification as the safest practice to ensure GDPR compliance, with the relevant Annexes appropriately filled in.

SCC clauses can be added to and built into contracts that also include agreements on other contractual elements. However, if used, the SCC wordings cannot be modified but must be included without modification to remain valid.

It is the processor's responsibility to ensure that the contractual provisions agreed on with the client are also implemented in the contractual agreements with the LSP's suppliers, service providers and subcontractors.

Due to the diverging practices, and continued uncertainty around the content in contractual agreements within the T&I sector, the TEW expert panel would welcome sector-specific Standard Contractual Clauses as a tool for promoting uniform and consistent standards of cooperation between market players, where data processing is concerned. Standard clauses would give both freelancers and language service companies the legal and organisational certainty they seek when

entering in a business contract under which personal data are processed.

### *International data transfers*

Within the T&I sector, personal data is routinely transferred to third countries. These transfers, albeit routine for LSPs and necessary for carrying out translation activities, require the controller's approval.

Transfers to third countries can be contractually agreed using Standard Contractual Clauses for transfers of personal data.

However, some grey areas remain in the scope of transfers to third countries, for example, whether data hosted on an EU server or cloud-based tool is indeed transferred to a third country when it is securely accessed by a translator in a third country, but remains stored in the EU at all times. The T&I sector shares these aspects with many IT sectors, and the TEW expert panel recommends further exploration of established interpretations and guidelines which could be directly applied to the T&I sector.

### *Further issues around contractual agreements and obligations of the processor*

The TEW expert panel wishes to draw attention to a few specific further issues encountered in the course of this project.

#### **Contract in writing**

The GDPR's national translations on the form of contractual agreements diverge. This has resulted in different interpretations of what the GDPR's requirement of 'The contract or act shall be in writing, including in electronic form' means.

The TEW expert panel adheres to the interpretation that the GDPR does not require a client's signature to render a contract valid, but allows for electronic forms, for example, a confirmation via email.

#### **Legal basis for processing**

The TEW expert panel notes that in order to process client data, an LSP does not need to define a legal basis for this processing.

As a processor has no direct relationship with data subjects, they therefore do not base the processing on one of the legal bases of Article 6 in the GDPR. The controller should ensure the lawfulness of the processing in the direct relationship with the data subject, and establish the legal basis for processing. The established legal basis enables the controller to legally pass on the personal data for processing to the processor.

#### **Audits**

The TEW expert panel has noted another grey area in the application of the GDPR within the T&I supply chain, namely the obligation laid down in Article 28 on audits conducted by the controller,

and the extent of access processors and sub-processors are obliged to grant for such audits.

The TEW expert panel advises against Data Processing Agreements which contain very general clauses providing the controller full, all-inclusive access to the premises and data processing equipment of the processor or sub-processor. The panel recommends for the scope of any audit or inspection to assure confidentiality of all data, repositories, and documents not relevant to the data processing carried out for the specific client-controller.

# Use of sub-processors

## Use of sub-processors summary

A supply chain consisting of an LSP-processor and their LSP-sub-processors is one of the specific features of the T&I sector.

The GDPR states that if a data processor plans to engage a sub-processor to carry out processing on its behalf, it must obtain prior specific or general written authorisation from the data controller.

For LSPs, this means that they must obtain the client's consent to sub-contract processing activities, and that they are responsible for their suppliers' activities and GDPR compliance.

## TEW expert panel's conclusions

A major grey area in the application of an LSP-processor's obligations under the GDPR has been the meaning of a controller's 'prior specific or general written authorisation' when applied to a T&I context.

Before the publication of the new SCCs in 2021, the concept of 'general permission' was largely interpreted in the T&I sector as permission to use sub-processors, and defined categories of sub-processors in general, without listing them by name in the data processing agreement.

However, in the TEW expert panel's view, clauses in the new SCCs between controllers and processors leave no room for ambiguity. **To comply with their obligations under the GDPR, an LSP should list the sub-processors they are planning to use to perform their services and data processing activities.**

The TEW expert panel acknowledges that this new interpretation has far-reaching adverse effects on the business activities of LSPs as processors and sub-processors, and compliance to it can be very difficult.

It is clear that with such a complex, momentous new interpretation, **further guidance for the T&I sector is required to clarify how LSPs engaging subprocessors may fulfil their obligations in practice.**

## Resources

[Standard Contractual Clauses between controllers and processors](#)

# Use of sub-processors

## Use of sub-processors analysis

A supply chain consisting of an LSP-processor and their LSP-sub-processors is one of the specific features of the T&I sector. Due to the ad hoc nature of translation and interpreting assignments, LSP-processors may maintain vendor databases of suppliers who can translate into a multitude of different languages, with different competencies and qualifications.

GDPR Article 28(2) states that if a data processor plans to engage a sub-processor to carry out a portion or all of the processing on its behalf, it must obtain 'prior specific or general written authorisation' from the data controller.

Where an LSP acting as a processor engages a sub-processor, the same data protection obligations as set out in the contract between the controller and the LSP apply to the sub-processor, in particular by providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDPR.

Where a sub-processor fails to fulfil its data protection obligations, the LSP as the initial processor remains fully liable to the controller for the performance of the sub-processor's obligations.

For LSPs, this means that they must obtain the client's permission to sub-contract processing activities, and that they are responsible for their suppliers' activities and GDPR compliance. The TEW expert panel recognises that this is one of the most challenging areas of GDPR compliance in the T&I sector.

### *Lists of sub-processors*

A major grey area in the application of this obligation has been the meaning of the controller's 'prior specific or general written authorisation' when applied to a T&I context.

Before the publication of the new Standard Contractual Clauses in 2021, the concept of general permission was largely interpreted in the T&I sector as permission to use sub-processors, and defined categories of sub-processors in general, without listing them by name in the data processing agreement.

However, the TEW expert panel notes that these concepts have now been further clarified in the new Standard Contractual Clauses between controllers and processors, where Article 7.7 on the use of sub-processors clarifies as follows:

*OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.*



*OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least [SPECIFY TIME PERIOD] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.*

In choosing the right approach, LSPs should pay special attention to the above Clause 7.7 of the SCCs. The list of authorised sub-processors should be agreed upon signing the SCCs and where the authorisation is chosen to be specific, this list should also be included in Annex IV.

For an LSP, this means listing all sub-processors the LSP is planning to use to perform their services and data processing activities.

This list of sub-processors should include not only a list of subcontracted LSPs, but also a list of other service providers, such as providers of machine translation and CAT tools, accountants, e-mail providers, etc.

In a typical T&I supply chain, this would also mean that all sub-processors should pass on to the processor above them a list of all sub-processors they intend to use.

The TEW expert panel acknowledges that this new interpretation has **far-reaching adverse effects** on the business activities of LSPs as processors and sub-processors, and compliance to it can be very difficult, if not impossible.

For an LSP, a list of possible sub-processors that could conceivably be engaged in carrying out an assignment essentially corresponds to their entire vendor database of freelance translators and interpreters and language service companies. That database may contain hundreds, even thousands of names of linguists, who may or may not process data for a particular client as the LSP's sub-processor. Naturally, these individuals are themselves also data subjects, whose data is now shared with a large number of clients – purely because they might at some point in the future become sub-processors of the client's data.

Sharing lists of sub-processors also poses a significant business confidentiality risk for LSPs, as it involves the disclosure of restricted company knowledge, and may result in the knowledge being shared with direct competitors. Moreover, lists of an LSP's possible sub-contractors never remain static, as new sub-processors are added, and others removed, which would necessitate constant updating of the list of sub-processors approved by the client.

It is clear that with such a complex, momentous new interpretation, further guidance for the T&I sector is required, and the TEW expert panel calls for clarity and further exploration on how in practice LSPs may fulfil their obligations as processors when it comes to GDPR Article 28(2), and SCC Article 7.7, without seriously and adversely jeopardising their business activities, and without unduly compromising business confidentiality.

# Data retention

## Data retention summary

Under the GDPR, data cannot be stored indefinitely, but needs to be erased after a defined period of time, the data retention period.

Administrative data should not be retained longer than necessary, but it can and should be kept for as long as Member State Law requires or allows for the exercise of relevant legal claims.

Data in translated or interpreted content is subject to data retention periods defined either by the controller, or by Member State Law. As local national regulations diverge, for example, on storing sworn or state-authorised translations, the application of Member State law should be assessed on a national level.

## TEW expert panel's conclusions

**If no Union or Member State Law requires an LSP to retain personal data for a specific period of time, an LSP-processor, and their sub-processors, should delete or return the data at the choice of the client-controller after the end of the provision of services relating to the processing.**

**The TEW expert panel advises LSPs to consider extending the scope of translation and interpreting services, to allow for data retention for a reasonable – but still definite – period of time in order to ensure the full and complete completion of services.**

To facilitate the tracking of data retention periods, the TEW expert panel calls on developers of Translation Management Systems to put in place functions to allow LSPs to implement, track and comply with relevant data retention periods.

A critical issue in the T&I profession is data retention within translation memories, and the common practice of retaining original and translated data in translation memories (TMs) for the purposes of further re-use.

The TEW expert panel sees that the act of retaining personal data in translation memories, including those with legacy data, constitutes a type of processing that is not conducted in the course of processing on behalf of the client as a controller.

**In the TEW expert panel's view, by retaining data in a TM, an LSP becomes a controller of that data, with all the associated obligations.**

The TEW expert panel recommends data anonymisation as a powerful mechanism to remove personal data and to mitigate GDPR risk in TMs and other data repositories, but notes that anonymisation does not guarantee full erasure of all personal data, and hence full compliance with the GDPR.

# Data retention

## Data retention analysis

Data retention under the GDPR is governed by the principles of purpose limitation, storage limitation and data minimisation.

Data cannot be stored indefinitely, but needs to be erased after a defined period of time, the data retention period.

As a data controller for administrative client, supplier, and employee data, an LSP is comparable to any business, and should ensure that it is compliant with the GDPR and local laws specifying data retention periods.

Administrative data should not be retained longer than necessary for the purposes for which it was collected, but it can and should be kept for as long as Member State Law requires or allows for the exercise of relevant legal claims.

To facilitate the tracking of data retention periods, the TEW expert panel calls on the developers of Translation Management Systems to put in place functions to allow LSPs to implement, track and comply with relevant data retention periods for client and supplier administrative data.

### *Retention of translated or interpreted content*

Data in translated or interpreted content is subject to data retention periods defined either by the controller, or by Member State Law.

According to Article 28(3)(g) of the GDPR, the processor,

*at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.*

The TEW expert panel notes that, as national regulations in each Member State diverge, for example, on storing sworn or state-authorized translations, the application of Member State law should be assessed on a national level.

If no Union or Member State Law requires an LSP to retain personal data, the LSP-processor should delete or return the data at the choice of the controller after the end of the provision of services relating to the processing.

In the context of this TEW GDPR project, the expert panel considered a number of issues.

The provision of translation and interpreting services is often understood to extend to the delivery of a translated document or the end of an interpreting assignment, with an associated data retention period.

This, however, may prevent the LSP from modifying deliverables based on client feedback or correcting mistakes. It also leaves the LSP open to vulnerabilities in terms of technical issues around deliverables, challenging non-payment, or maintaining records for potential liability claims.

The TEW expert panel advises LSPs to consider extending the scope of translation and interpreting services, to allow for data retention for a reasonable – but still definite – period of time in order to ensure the full and complete completion of services.

When defining the scope of services offered, the expert panel further advises LSPs to carefully analyse which extended purposes are in the interests of the client, and which purposes may tilt the LSP on the side of becoming a controller of the data, with all of its associated obligations.

For example, although Article 17(3)(e) of the GDPR concerning the right of erasure allows personal data to be retained for the ‘exercise or defence of legal claims’, as a processor, an LSP cannot refer to the exception provided for in the provision of this Article, which relates to the obligations of the controller.

### *Establishing data retention periods*

The TEW expert panel recommends the following steps in scoping out, setting, and complying with appropriate data retention periods for personal data in translated or interpreted content, agreed between the client-controller and LSP-processor.

- Identify whether any Union or Member State Law overrides client data retention periods.
- Assess the risk of prolonged data retention.
- Define the elements included in the provision of service, such as the possibility to issue copies, make adaptations, or rectify errors.
- Apply appropriate technical and organisational measures to safeguard retained data.
- Ensure the data retention period is adhered to throughout the supply chain.
- Assess the consequences of data retention for the LSP’s further purposes.
- Erase/anonymise the personal data after the defined data retention period.

The TEW expert panel sees a clear need for best practice and standard terms for data retention in data processing agreements for the T&I profession to protect the interests of clients and LSPs, as well as the data subjects whose personal data is being processed.

### *Data retention in translation memories*

A critical issue in the T&I sector is data retention within translation memories, and the common practice of retaining original and translated data in TMs for the purposes of further re-use. These TMs frequently contain both data collected prior to the GDPR coming into force, and after it.

In the TEW expert panel’s view, the act of retaining the personal in translating memories, including

those with legacy data, constitutes a type of processing that is not conducted in the course of processing on behalf of the client as a controller.

As such, by retaining data in a TM for its own purposes, an LSP becomes a controller of that data, with all the associated obligations.

The TEW expert panel acknowledges that translation memories are one of the most valuable business assets of an LSP. As such, it is in the interests of the T&I sector to find ways to mitigate the risks that TMs as data repositories pose.

Current technical measures are not 100% capable of removing all traces of personal data, but they provide powerful ways of mitigating GDPR compliance risks through scrambling data, and anonymising personal data in TM repositories.

The way personal data is stored in a translation memory is, in itself, relatively secure. To open a translation memory, special software or access is required, and the data are 'shredded' in small segments. However, unless personal data is removed or reliably anonymised, it is retained in the translation memory for an indefinite period, a practice not permitted under the GDPR.

As a specific note, it is the TEW expert panel's opinion that any data retention practices and periods should also be applied to data collected before the GDPR came into force.

### *Data anonymisation*

The TEW expert panel notes that in terms of GDPR compliance, the obligation to delete or return data only extends to the personal data in any translated or interpreted content.

As such, there is no requirement for a processor or sub-processor to delete entire documents or data repositories at the end of a data retention period, unless other contractual agreements require them to do so, and provided that the personal data can be deleted.

The TEW expert panel recommends data anonymisation as a mechanism to remove personal data and to mitigate GDPR risk in TMs and other data repositories.

The expert panel notes that, as a mechanism, anonymisation is a form of data processing, and as such should be authorised by the controller.

Existing automatic anonymisation solutions may reach an accuracy level of up to 95%, entirely dependent on the technology used, and the complexity of the data anonymised. This means that some personal data will remain, and that anonymisation does not guarantee full erasure of all personal data, and hence full compliance with the GDPR.

The TEW expert panel therefore recommends for automated anonymisation to be followed by human anonymisation to check and/or to improve the anonymisation result. In some content involving complex types of personal data, or with types of documents that do not lend themselves to anonymisation, it may, however, be more expedient to consider deleting the whole document rather than attempting to erase personal data.

# Risk mitigation

## Risk mitigation

Some European data protection authorities and organisations involved in the data protection arena are increasingly exploring risk-based assessments to increase levels of GDPR compliance, and to facilitate the implementation of the GDPR's requirements.

The risks involved in processing personal data in translated or interpreted content – for data subjects' rights and freedoms, but also for LSPs' business activities – can be significantly mitigated through a robust risk-based approach.

In the T&I sector, the *GDPR and personal data in translation* guide explores practical ways of identifying, assessing, and mitigating risks in the T&I supply chain.

An updated version of the guide was published in April 2022 by the European Union of Associations of Translation Companies and the UK's Association of Translation Companies, in collaboration with FIT Europe and the FreeLING Foundation. It is available online free of charge.

The foundations of a risk-based approach are rooted in an LSP's awareness of their obligations under the GDPR, and in their understanding of their unique operational practices.

On the road towards improved GDPR awareness and compliance in the T&I sector, the TEW expert panel advocates for an approach of documented risk and compliance assessment, and advises LSPs to:

- assess risks from the point of view of the LSP's own operations, identify and mitigate risks specific to the LSP's unique T&I activities;
- put in place appropriate contractual agreements with the controller, and throughout the supply chain;
- document risk assessments and personal data processing activities and the technical and organisational measures associated with them;
- ensure transfers to third countries are contractually agreed, and appropriately managed;
- put in place, track, and comply with defined data retention periods;
- involve all levels of the supply chain in raising awareness of their obligations, and achieving increased compliance.

## Resources

EUATC Guide GDPR and personal data in translation: <https://bit.ly/3vovy56>

# Conclusions and next steps

## Conclusions and next steps

Expert discussions preceding the Translating Europe Workshop, and the engagement with T&I professionals at the workshop, have crystallised into two clear insights:

- The T&I sector needs clear, unambiguous, sector-specific guidelines on the application and implementation of the GDPR.
- This TEW GDPR project has shone a light on, and resolved, some of the most challenging grey areas and issues the T&I sector faces, but specific topics require further exploration.

As T&I professionals, it is our responsibility to protect the rights and freedoms of the data subjects whose data we process, and to ensure that the GDPR is complied with at all levels.

The GDPR does not bend to our will, but neither is it there to prevent our global business activities, and our work in enabling international communication. We must accept our obligations as controllers, processors, and sub-processors, while continuing to provide a smooth, professional service.

This report outlines the findings of the TEW expert panel *Towards Common European GDPR Guidelines for the Translation and Interpreting Profession*. These are our first steps towards those guidelines, brought about by a collective willingness and effort to work together as a sector.

Our goal is to continue on this journey, and our next steps include applying for funding for a further Translating Europe Workshop, aimed at creating a set of GDPR guidelines for the T&I sector, drawing on the findings of this TEW GDPR project, and the emerging risk-based approaches of national data protection authorities.

**Raisa McNab**

GDPR Representative

European Union of Associations of Translation Companies (EUATC)

# Project partners

## Project partners

This Translating Europe Workshop *Towards Common European GDPR Guidelines for the Translation and Interpreting Profession* was funded by the European Commission Directorate-General for Translation, and carried out with the involvement of the following project partners:

[Dublin City University \(DCU\)](#)

[EUATC](#)

[FIT Europe](#)

[FreeLING Foundation](#)

[Irish Translator's and Interpreters' Association](#)

[Lublin Translators Association](#)

[Maria Curie-Sklodowska University \(UMCS\)](#)

[Polish Society of Sworn and Specialized Translators TEPIS](#)

[Translation Industry Employers Association POLOT](#)

[Pangeanic](#)



# Project experts

## Project experts

Project experts involved in this Translating Europe Workshop *Towards Common European GDPR Guidelines for the Translation and Interpreting Profession* include legal experts, language services professionals, and representatives of translator, interpreter, and language service company associations.

### **Stefanie Bogaerts**

Project leader

Stefanie Bogaerts is a Polish-Dutch Sworn translator living and working in Poland. She holds a degree in Eastern European Languages and Cultures from the University of Leuven, Belgium, and postgraduate degrees in public relations, multilingual business communication and management.

Stefanie is co-founder and president of the board of Fundacja FreeLING (FreeLING Foundation), a Polish non-profit organisation providing training for translators and interpreters. She is also a member of Lubelskie Stowarzyszenia Tłumaczy (Lublin Translators' Association) and is actively involved in legislative projects and campaigns to improve working conditions for translators.

### **John O'Shea**

Project leader

John O'Shea is a Greek-English translator specialising in legal translation. He holds Bachelor of Laws (LL.B.) and Master of Laws (LL.M) degrees from the Queen's University of Belfast, Ireland.

John is the Chairperson of FIT Europe, the European Regional Centre of the International Federation of Translators, representing professional translator and interpreter associations and practitioners across Europe. John is also an independent legal researcher, and the founder of Lex Graeca.

### **Małgorzata Dumkiewicz**

dr hab. Małgorzata Dumkiewicz is a legal counsel, research and didactic worker employed as Associate Professor at the Faculty of Law and Administration (the Chair of Commercial Law) at Maria Curie – Skłodowska University in Lublin, Poland.

Małgorzata is an author of publications in the field of company law and economic law.

**Manuel Herranz**

Manuel Herranz is CEO at Pangeanic, an NLP company with strong specialism in private Machine Translation and Anonymisation, providing solutions to government and enterprise. Prior to that he managed the language services arm of a Japanese B.I Corporation in Europe.

Manuel is a double graduate from Manchester University and has written or co-written over 10 academic papers on different NLP areas, from MT to building corpora and data-masking.

**Magdalini Skondra**

Magdalini Skondra is a Lawyer before the Greek Supreme Court, member of the Thessaloniki Bar Association and an Accredited Data Protection Officer Executive. She holds the internationally recognised certificate of Certified Information Privacy Professional/Europe (CIPP/E), from IAPP, the International Association of Privacy Professionals).

Magdalini is a graduate of the Aristotle University of Thessaloniki Law School and holds a Master of Science in Law and Informatics from the University of Macedonia and the Department of Law of the Democritus University of Thrace.

**Paweł Kamocki**

Dr. iur. Paweł Kamocki is a legal expert in Leibniz-Institut für Deutsche Sprache, Mannheim, Germany. He studied linguistics and law, and holds a Doctorate in Law from the universities of Paris and Münster.

Paweł is certified to work as an attorney in France. An active member of the CLARIN community, he currently chairs the CLARIN Legal and Ethical Issues Committee. He has also worked with other projects and initiatives in the field of research data policy (RDA, EUDAT) and co-created several LegalTech tools for researchers. One of his main research interests are legal issues in Machine Translation.

**Raisa McNab**

Raisa McNab is CEO at the UK's Association of Translation Companies (ATC). She holds a Master's Degree in Translation and Interpreting from the University of Turku, Finland.

Raisa is the GDPR Representative of the European Union of Associations of Translation Companies (EUATC). She is also the ATC's Lead on Standards, and oversees the operations and development of ATC Certification, a language services ISO Certification Body.

**Zoe Milak**

Zoe Milak is a staff translator for Italy's central bank, Banca d'Italia. She specialises in legal and financial translation, and has also worked as an attorney both in Italian and American law firms after graduating from the University of Chicago's Law School.

Zoe is a Qualified Member of Associazione Italiana Traduttori e Interpreti (AITI) and currently serves on its Regional Council (Lazio Division) as chair of the regional training programme committee. She is also an active member of the American Translators Association's Italian Division.

**Wojciech Wołoszyk**

Wojciech Wołoszyk is a lawyer-linguist, legal translator and reviewer of legal and EU translations, court expert in legal linguistics. He is the CEO of IURIDICO Legal & Financial Translations.

Wojciech is an author of articles on issues of terminology in legal translations, and on legal aspects of the language services industry, including intellectual property rights and public procurement. He is the Coordinator of the team of reviewers working on the English-Polish part of the World Law Dictionary, Member of the Expert Panel and of the Board at PT TEPIS, co-founder of and Member of the Board of POLOT (the Polish Association of LSPs).

# References

## References

[Recording of the Translating Europe Workshop Towards Common European GDPR Guidelines for the T&I Profession](#)

[General Data Protection Regulation \(GDPR\)](#)

[European Data Protection Board \(EDPB\) Guidelines on the concepts of controller and processor in the GDPR](#)

[Standard Contractual Clauses between controllers and processors](#)

[Standard Contractual Clauses for the transfer of personal data to third countries](#)

[CNIL guidance on processors processing data for their own purposes](#) (in French)

[International Association of Privacy Professionals' analysis of CNIL guidance](#) (in English)

EUATC Guide GDPR and personal data in translation: <https://bit.ly/3voyy56>