GDPR and personal data in translation

Published January 2021

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Association of Translation Companies

DEFINING STANDARDS OF EXCELLENCE

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Introduction

The EU's General Data Protection Regulation (GDPR) exists to protect people's personal data.

The GDPR's reach extends to all areas of business, for example, how companies collect, process and retain their employees', clients' and suppliers' personal data. Guidance and resources for handling this kind of data are widely available.

For the language services industry, the presence of personal data in content for translation poses unique challenges, for example:

- *It may not be possible to identify personal data in content for translation before it has already been sent to a language service company or a freelance translator, and its translation has begun, for example, due to the sheer volume of content for translation, the format in which it is provided, or because the project manager does not understand the source language.*
- *Clients may not be aware of GDPR implications when it comes to personal data in content for translation.*
- *Content for translation is transferred within the European Economic Area (EEA), and from EEA countries to multiple third countries for translation, which creates a complex web of processor relationships.*

These challenges can be addressed through a **robust risk-based approach**, so that handling personal data in content for translation forms part of your overall GDPR compliance process, whether you are an owner or manager of a language service company or a freelance translator.

This overview is intended as an aid to language service companies and freelance translators. It focuses on identifying the challenges around GDPR compliance when processing content for translation, and establishing a risk-based approach to facilitate GDPR compliance activities in relation to translated content.

At the end of this overview, you will find a Readiness Checklist which will help you to assess what contractual agreements and processes you may need to put in place, a flowchart for Contracts and Transfer Routes, and a flowchart for Risk Assessment by Content Type.

References and resources

At the time of writing, there is no authoritative European-wide GDPR guidance tackling the complexities of GDPR compliance within the language services industry.

European language industry associations including the EUATC and FIT Europe are working with experts and authorities with a view to establishing common European guidelines for the language services industry.

The overview uses authoritative sources, primarily the General Data Protection Regulation itself. Guidance from the United Kingdom's data protection authority The Information Commissioner's Office's extensive Guide to the GDPR has also been used as an easy-to-understand reference with GDPR compliance, still useable despite the UK's new status as a 'third country'.

Although the GDPR applies to all EEA countries, information provided by national data protection authorities may vary, and national data protection legislation may include other provisions you should be aware of, so you are advised to act with caution. Refer to your national data protection authority's guidance where available, and to any other national regulations which may link to the GDPR.

You can find a list of National Data Protection Authorities (members of the European Data Protection Board) here.

Note that nothing in this overview constitutes legal advice.

The overview has been funded by the European Union of Associations of Translation Companies (EUATC), with input and advice from FIT Europe in the context of a partnership the organisations have established. The overview has been jointly produced with the UK's Association of Translation Companies (ATC).

Table of Contents

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Key GDPR concepts and principles

The General Data Protection Regulation sets guidelines for the collection and processing of personal data from individuals who live in the European Union (EU). The GDPR also applies to the countries forming the EEA with the EU.

At the core of the GDPR is the concept of *data protection by design*. This means carefully assessing and designing processes so that they take into account and protect individuals' personal data, and documenting the decisions made and processes put in place.

The key principles of the GDPR are *lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability*.

Personal data

Personal data is information that relates to an identified or identifiable person, *a data subject*. Identifiable information could be, for example, their name or personal identification number. If it is possible to identify the individual directly from other information, that information may also be personal data.

Special category data is personal data that requires more protection because it is sensitive. Special category data is, for example, data concerning health, racial or ethnic origin, political opinions or religious beliefs.

Rights of the data subject

The GDPR provides the following rights for individuals in connection with their right to the protection of personal data.

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Roles of controller and processor

The roles of *controller* and *processor* are key concepts in the GDPR.

Controllers have the overall control over the purposes and means of the processing of personal data.

Processors act on a client's instructions, and may not have purposes of their own for processing the data, even if they make some technical decisions about how they process the data.

Controllers' and processors' responsibilities and obligations vary, and in business contexts, your role will depend on the situation.

For example, a language service company will typically be a:

- controller when processing client and client employee data;
- controller when processing their employee and supplier data; and
- processor when processing data in content for translation received from their clients.

Legal basis for processing

For each type of processing or relationship, the data controller should establish and document a legal basis for processing personal data.

There are six legal bases for processing personal data.

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Some of the above legal bases for processing personal data are largely irrelevant for language service companies and freelance translators. For controlling client, employee and supplier data, “Contract” and “legitimate interests” are the most commonly used legal bases. “Consent” as a legal basis should be considered carefully and used with caution.

When it comes to personal data in content for translation, it is the responsibility of the data controller to define the legal basis for processing.

Inside and outside the EEA

The GDPR *primarily* applies to controllers and processors located in the EEA. It establishes a regulatory basis for ensuring that personal data is protected within the EEA, but it also applies when that data is transferred elsewhere for processing.

As individuals within the EEA risk losing the protection of the GDPR if their personal data is transferred outside the EEA, the GDPR includes restrictions on transfers of personal data outside the EEA.

As such, the GDPR also concerns controllers and processors outside the EEA when they are processing personal data originating from the EEA.

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Personal data in content for translation

In terms of GDPR compliance, the language services industry faces a number of unique challenges in processing personal data in content for translation.

'Incidental' personal data

Unlike when processing personal data relating to a client or an employee, the personal data present in content for translation is *incidental*.

The objective of the translation assignment is to translate content from one language to another. Within that process, should the content happen to include personal data, it is important to protect that data.

The challenge is that the presence of personal data may at times not be identified until translation has already begun, for example, due to the sheer volume of content for translation, the format in which it is provided, or because the project manager does not understand the source language.

No visibility on data origin

Often, we have no visibility at all over where the personal data in content for translation comes from; whether it originates from within the EEA or not, who the original controller collecting the data is, and so on.

The client may be unaware that there exists personal data in their content for translation, or that the GDPR extends to this type of 'incidental' processing of personal data in the same way as it does to the more typical types of data processing.

A global activity

Translation by nature is a global activity, and content for translation is frequently transferred outside the EEA for processing, that is, for translation into another language. As the GDPR places restrictions on the transfer of personal data outside the EEA, it is important to consider how best to protect that data.

Ad hoc assignments

Translation assignments are often carried out on an ad hoc basis, in a translation supply chain between clients, language service companies and freelance translators. Within these kinds of supply chains for ad hoc work, it is difficult to control the individual roles and responsibilities without excessive contractual paperwork.

Our responsibility

Because of these challenges, and because of the absence of authoritative guidance specific to the language services industry, this overview focuses on identifying areas within which we are able to influence the processing of personal data in content for translation and protect the data subjects whose data we process.

At the heart of this approach is our responsibility towards our clients, suppliers and the data subjects themselves. Regardless of the challenges in processing personal data in content for translation, we have a hugely important role to play in identifying the risks involved in processing and transferring personal data.

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Translation supply chain roles and responsibilities

A typical translation supply chain may consist of the following actors:

When assessing and defining the roles of controller and processor, the main question to ask is who controls the data, determines the purposes for which the data are processed, and the means of processing?

In this overview, we make reasonable interpretations of the typical roles in the translation supply chain, in the absence of authoritative guidance specific to the language services industry.

Controller, Processor or Sub-Processor?

When defining relationships within the translation supply chain, the roles of Controller, Processor or Sub-Processor should be assigned clearly.

The client

In a typical supply chain, the client

- may have collected the personal data sent for translation;
- decides what the purpose or outcome of the processing is to be;
- defines the legal basis for processing the personal data;
- obtains benefit from the processing;
- has autonomy as to how the personal data is processed; and
- appoints a processor to process personal data on their behalf.

→ The client is a Controller.

The language service company

When determining the language service company's role within the chain, we can assume that they

- are following instructions from the client regarding the processing of personal data;
- are given the personal data by the client;
- do not decide to collect personal data from individuals;
- do not decide the legal basis for the use of that data;
- do not decide what purpose(s) the data will be used for; and
- are not interested in what the end result of the processing will be used for.

→ The language service company is a Processor.

In this Controller-Processor relationship, although the language service company as a Processor may make some decisions on how data is processed, for example, which translation technology tool to use, or which translator to use, these decisions are implemented under a contract with the client.

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

The freelance translator

The role of a freelance translator depends on where they are within the chain:

- When working for a direct client, the freelancer is a Processor.
- When working for a language service company (the Processor), the freelancer is a Sub-Processor.

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Contractual agreements

The GDPR requires *data controllers* to ensure the protection of personal data. Controllers must be able to demonstrate that the processors they engage, and the sub-processors their processors engage, protect personal data and act in compliance with the GDPR.

The relationship and data processing activities between a controller and a processor must be contractually agreed on, as defined in the GDPR.

The GDPR sets out what needs to be included in a controller-processor contract:

- Subject-matter and duration of the processing
- Nature and purposes of the processing
- Type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject.

After the completion of the processing, the processor should, *at the choice of the controller*, return or delete the personal data, unless there is a requirement to store the personal data under EU or Member State law to which the processor is subject.

You can find more information on contractual agreements in the UK Information Commissioner's Office ICO's GDPR Guide here. The Guide also includes direct links to the relevant GDPR clauses.

Using sub-processors

A processor should not engage another processor (a sub-processor) without the controller's prior specific or general written authorisation.

Processors should put in place contractual agreements with the sub-processor, imposing the same GDPR obligations on the sub-processor as agreed between the controller and the processor.

This should include requirements for the sub-processor to provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the GDPR's requirements.

The wording of these obligations does not need to exactly match those set out in the contract between the controller and the processor, but should offer an equivalent level of protection for personal data.

Data Processing Agreement

A Data Processing Agreement (DPA) is a type of contractual document between a controller and a processor, or a processor and a sub-processor. It sets out the relationship between the controller and the processor or the processor and sub-processor, and the specifics of data processing.

The GDPR does not specify the format of a DPA, nor whether it should be a separate contract from an existing contractual agreement between the controller and the processor, or processor and sub-processor.

A sample Data Processing Agreement can be found here.

Standard Contractual Clauses

Standard Contractual Clauses (SCCs) are a mechanism to contractually govern the transfer of personal data outside the EEA.

To date, the European Commission has issued two sets of SCCs: *from EU data controller to non-EU or EEA controller*, and *from EU data controller to non-EU or EEA processor*.

For example, a client-controller based in France should put in place SCCs with a language service company processor based in India.

Existing SCC wording cannot be deviated from but must be included in the contract as is.

You can find the SCC templates here.

The UK's data protection authority ICO has an interactive tool to help select, understand and complete the right SCCs for a controller-processor relationship from the point of view of EEA-to-UK transfers, but it can also be used in other EEA-to-third-country situations. You can find the tool here.

Unfortunately, no SCCs currently exist to govern the relationship between a processor and a sub-processor when transferring personal data outside the EEA.

Contractual agreements in the translation supply chain

The flowchart on Contracts and Transfer Routes in Annex II of this overview may help you identify the contractual agreements needed in your translation supply chain.

In practice, managing contractual agreements for GDPR purposes in the translation supply chain may be challenging, if

- the controller does not put in place an appropriate contractual agreement with the processor; or if
- there are multiple processors and sub-processors in the chain in different parts of the world.

You may be able to mitigate the risks associated with contractual agreements within the translation supply chain by ensuring that the controller is aware of and has authorised the use of sub-processors and the transfer of their data outside the EEA.

Data transfers

As controllers, processors and sub-processors in the EEA all have to comply with GDPR requirements, no specific measures beyond the basic contractual agreements are required for transferring data within the EEA.

The European Commission may also determine other countries as having adequate levels of data protection. Transfers of personal data to 'adequate countries' also do not require specific measures or authorisation. You can find a list of adequate countries here.

For the rest of the world, when personal data is transferred outside the EEA and adequate countries to 'third countries', appropriate contractual safeguards such as Standard Contractual Clauses should be put in place.

The flowchart on Contracts and Transfer Routes in Annex II of this overview may help you to identify what contractual agreements for different transfer routes are needed in your translation supply chain.

Risk assessment

The GDPR includes provisions for evaluating risks to the rights and freedoms of data subjects based on an objective assessment of the likelihood and severity of the risks, with reference to the nature, scope, context and purposes of the processing. This evaluation should establish whether data processing operations involve a *risk* or a *high risk* to the rights and freedoms of data subjects.

The GDPR asserts the controller's responsibility and liability for any processing of personal data carried out by them, or on their behalf. It obliges the controller to implement appropriate and effective measures to mitigate the risk, and to be able to demonstrate the compliance of processing activities within the GDPR.

However, as the providers of a specialist service, the processors and sub-processors in the translation supply chain have a responsibility towards the controller, and the data subjects whose data they process, to identify and mitigate particular risks associated with translation activities.

There are three key areas within which processors and sub-processors in the translation supply chain can help risks to data subjects' rights and freedoms from arising.

- Contractual compliance throughout the supply chain
- Identifying and mitigating risks particular to translation activities
- Documenting risk assessments and personal data processing activities

In this overview, we identify risks particular to translation activities, and consider how to mitigate them.

Specifically, we consider risks around:

- contractual agreements
- data transfers
- content types
- data retention
- data protection.

Every language service company's and freelance translator's operations are unique, and you should consider the risks around processing personal data in translation content in the context of your operations.

When assessing your operations specifically for the processing of personal data in translation content, keep at the forefront of your mind the GDPR's purpose of protecting individuals' personal data. Consider whether in your operations there are areas which may pose a risk to the rights and freedoms of those individuals.

In practice, your risk assessment may consist of reviewing your existing processes, documentation and contractual agreements, identifying any gaps or particular risks, and considering how to address them.

This overview, along with the Readiness Checklist in Annex I as well as the flowcharts Contracts and Transfers in Annex II and Risk Assessment by Content Type in Annex III, may help you to assess your operations and any areas of risk you should pay particular attention to.

Documentation

The GDPR requires processors to keep records of processing activities carried out on behalf of a controller, including details of the controller, categories of processing, and transfers of personal data to third countries.

In practice, translation assignments are typically recorded in detail and compliance to the above is simple to demonstrate. In addition, the GDPR requires processors, where possible, to have general descriptions of technical and organisational safety measures.

In the context of the specific risks associated with the translation supply chain, and to be able to demonstrate compliance with the GDPR, consider documenting your risk assessment and any appropriate measures and safeguards you put in place.

Assessing and mitigating risk: contracts and data transfers

In the spirit of key GDPR principles of *fairness*, *transparency*, and *accountability*, you may wish to assess the risks around contractual agreements and data transfers, applicable in your circumstances, and apply a risk-based approach to mitigate them. Document your risk assessment and any appropriate safeguards you put in place.

When carrying out your risk assessment, you may wish to consider the following questions.

Is the controller aware that content they send for translation contains or may contain personal data?

If the controller is not aware of personal data in content for translation, they are unlikely to have considered the associated GDPR implications.

Consider how to raise the controller's awareness of their obligations when it comes to personal data in content for translation.

In addition, consider how you may ensure that the controller's awareness extends to all data repositories which may contain personal data, for example, translation memories as well as documents for translation.

Is there a controller-processor agreement in place?

If there is no agreement in place setting out the nature of the controller-processor relationship and how personal data is handled, there is a risk in terms of your ability to comply with the GDPR.

Consider how to put in place appropriate contractual agreements and safeguards for processing personal data in content for translation. Are you able to include appropriate contractual elements and safeguards in your own Terms & Conditions with the controller?

Are you likely to transfer content for translation to 'third countries'?

If your typical supply chain involves transferring content for translation to 'third countries', appropriate contractual agreements and safeguards for that should be put in place.

Consider how to contractually agree transfers to 'third countries' with the controller, taking into account the level of risk associated with the type of content being transferred.

Is there an appropriate processor-sub-processor agreement in place?

If the contractual agreement between the processor and the sub-processor does not ensure that personal data is processed down the supply chain in the way the controller requires, the processing may be in breach of GDPR, and the processor liable.

Consider how to contractually ensure that when transferring data within the EEA, or to 'adequate countries', or to 'third countries', any personal data in content for translation is protected in compliance with GDPR and the requirements of the controller.

EUROPEAN UNION OF ASSOCIATIONS OF TRANSLATION COMPANIES

Content profiling

Profiling content for translation and assessing risks based on the types of data you process may allow you to apply appropriate safeguards and mitigate the risks around processing personal data in content for translation, and to build GDPR compliance processes according to the level of risk.

Document your content profiling and risk assessment as part of your GDPR compliance process, in the spirit of key GDPR principles of *transparency* and *accountability*.

Risk profiling based on content type

Risk profiling based on the types of content you process allows you to closely examine and categorise any risk associated with typical content, for example, by domain, text type, client or end-client.

As you profile content types, you may discover clear areas of risk associated with certain types of content, and perhaps no risk with other content. You will be able to apply different types of safeguards depending on the level of risk.

The Risk Assessment by Content Type in Annex III of this overview may help you to carry out a risk assessment by content type, and to mitigate any risks based on content type.

Levels of risk by content type

No personal data | No risk

If the content for translation contains no personal data, there is no GDPR-related risk and no GDPR compliance implications.

For content for translation that doesn't contain any personal data, there are no GDPR-related restrictions on data transfers.

Non-sensitive personal data | Potential for low risk?

If the content for translation contains non-sensitive personal data, it's still classified as personal data.

As such, the GDPR applies, but the potential risks associated with processing it may be considered lower than that of the potential risks associated with processing sensitive personal data.

Sensitive personal data | Potential for high risk?

If the content you translate contains sensitive personal data, a special category under GDPR, it must be processed with caution and with due consideration to the potential risks to the rights and freedoms of the data subjects.

Assessing and mitigating risk: content types

Some of the below actions may be useful for you in assessing and mitigating the risks associated with processing content for translation containing personal data.

Identifying personal data

One of the main risks associated with processing personal data in content for translation is that it may not always be possible to even identify the presence of personal data until the content has already been transferred and is being translated.

Consider what types of content you typically process, what levels of risk can be associated with each type of data, and how personal data can be identified in different types of content.

Profiling content in translation for the level of risk associated with certain types of *typical content* and having a process to flag personal data in *content processed ad hoc* are ways to mitigate risk: by having a robust identification process, you are able to manage content containing personal data with due concern to the level of risk it presents.

Flagging content

Depending on the extent of the contractual agreements you have in place with the controller, once you have a process in place to identify personal data, consider whether you also need to specifically flag the presence of such data to the controller, and if so, how and when.

Pre-processing content

Depending on the types of content for translation you process, it may be possible to pre-process content ahead of transferring and translating it.

Mechanisms for mitigating risk through pre-processing may include redacting or pseudonymising personal data that does not require translation (e.g. names or ID numbers in certificates), and reinstating it after translation, where possible.

Retention of content based on risk level

Another mechanism to mitigate risk is to control the retention times of content based on its risk level, all through the translation supply chain.

For example, if high-risk content for translation is transferred outside the EEA with the client's approval, can you further mitigate the risk associated with the transfer by having a retention period shorter than that for content with no or low risk?

The role of translators

Within the translation supply chain, translators play a hugely important role in processing personal data securely and complying with data retention times.

Consider how best make translators aware of their role, involve them in the process, and ensure their compliance to GDPR and any contractual obligations.

Data protection

The GDPR places importance on the security of processing personal data, and this includes provisions for secure data protection and transfer.

Consider how you can ensure that the data you and your sub-processors handle remains safe, through implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Remember to consider the different stages personal data in content for translation goes through.

- Transfer from controller to processor
- Processor's data repositories
- Transfer from processor to sub-processor
- Sub-processor's data repositories
- Transfer from sub-processor back to processor and controller

For example, technical measures might include encryption of data in transfer, and organisational measures might include stricter restrictions for accessing high-risk data.

Data retention

Data retention refers to the amount of time personal data is kept before it is returned to the controller or destroyed, in line with the GDPR principle of *storage limitation*.

In short, the GDPR mandates that personal data should not be kept longer than needed. However, it doesn't set specific time limits for data retention.

Data retention periods should be agreed on in the Data Processing Agreement or other relevant contractual agreements.

Any data retention periods set by the controller must be adhered to all through the supply chain, both by the processor and any of their sub-processors.

Assessing and mitigating risk: data retention

A considerable risk within data retention lies in retaining personal data indefinitely because no appropriate retention periods have been set, or because data retention periods are not being adhered to.

Consider what processes should be put in place to comply with the agreed data retention periods and how to contractually agree and manage them with your sub-processors.

The simpler the data retention principles are, the easier they are to manage and adhere to.

Consider the following questions.

What data do you retain or destroy?

The GDPR only concerns personal data, so one of your first considerations should be around what data you will actually retain or destroy.

Consider whether it's appropriate and meaningful for you to destroy *all* of the content for translation at the end of the retention period, or put in place a process to destroy the personal data in content for translation *only*.

Your decision may depend on the type of content you process, and the level of risk associated with the personal data in that content. Some types of content will inevitably contain more personal data than others, and it may be very difficult to delete personal data *only*

in content where there are many different types or instances of personal data.

Has the controller set a retention time?

If so, this should be adhered to.

Consider what processes should be put in place to ensure that a specific controller's data is destroyed after the data retention period they have set comes to an end.

For example, are you able to flag or segregate a specific controller's data for destroying at the end of the retention period, away from other data?

What retention times are appropriate?

The GPDR does not stipulate how long retention periods should be.

Retention times specified by the data controller must be adhered to, but if you have an opportunity to discuss retention times with the controller, you may wish to consider what retention times are appropriate based on the levels of risk by content type, or where the content is transferred.

Specifically, you may wish to discuss retention times in the light of any contractual obligations between you and your client. For example, consider whether it's appropriate and possible to retain data until payment for the translation assignment has been received.

Where is the data stored?

When considering your data retention processes, ensure that they encompass all locations where data is stored. For example, not just in your internal folders, but potentially also on online data sharing platforms or in email attachments.

Put in place processes ensuring that data is destroyed everywhere it exists at the end of the retention period.

How to ensure compliance across the supply chain?

Ensuring data retention compliance across the supply chain is a critical link in protecting personal data.

Consider how you ensure compliance with your sub-processors, for example, by:

- agreeing clear data retention periods contractually;
- flagging data retention times with the sub-processor;
- reminding the sub-processor to destroy data at the end of the retention period; and
- checking that data has been duly destroyed.

What about translation memories?

Translation memories are one of the most valuable assets for any language service company or freelance translator.

Consider whether you may be able to help protect personal data in content for translation without destroying TM content, and to what extent, for example, by:

- using your software's personal data anonymiser tool; or
- redacting or pseudonymising personal data in pre-processing.

Check with your translation technology provider what tools or methods for anonymising they may support, but note that none of the technical methods described above, or other similar ones, will in all likelihood be fool-proof. Consider their use in the context of your overall risk assessment.

Conclusion

Although there is no authoritative advice specific for these challenges around processing personal data in content for translation, the basic principles of GDPR will guide you in implementing a sound GDPR policy, and carrying your responsibility as a processor or sub-processor.

The foundation of the GDPR is in data protection by design – building your processes to protect the data subjects whose personal data you process.

Once you have put in place appropriate contractual agreements, processes and documentation, review them regularly and improve them continuously.

Resources

General Data Protection Regulation (Directive 95/46/EC), including options for multilingual display: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

List of National Data Protection Authorities (members of the European Data Protection Board): https://edpb.europa.eu/about-edpb/board/members_en

UK's Information Commissioner's Office's (ICO) Guide to the General Data Protection Regulation (GDPR): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

GDPR.eu, a resource for organisations and individuals researching the GDPR, co-funded by the Horizon 2020 Framework Programme of the European Union: https://gdpr.eu/

Annexes

ANNEX I: Readiness Checklist

ANNEX II: Contracts and Transfer Routes

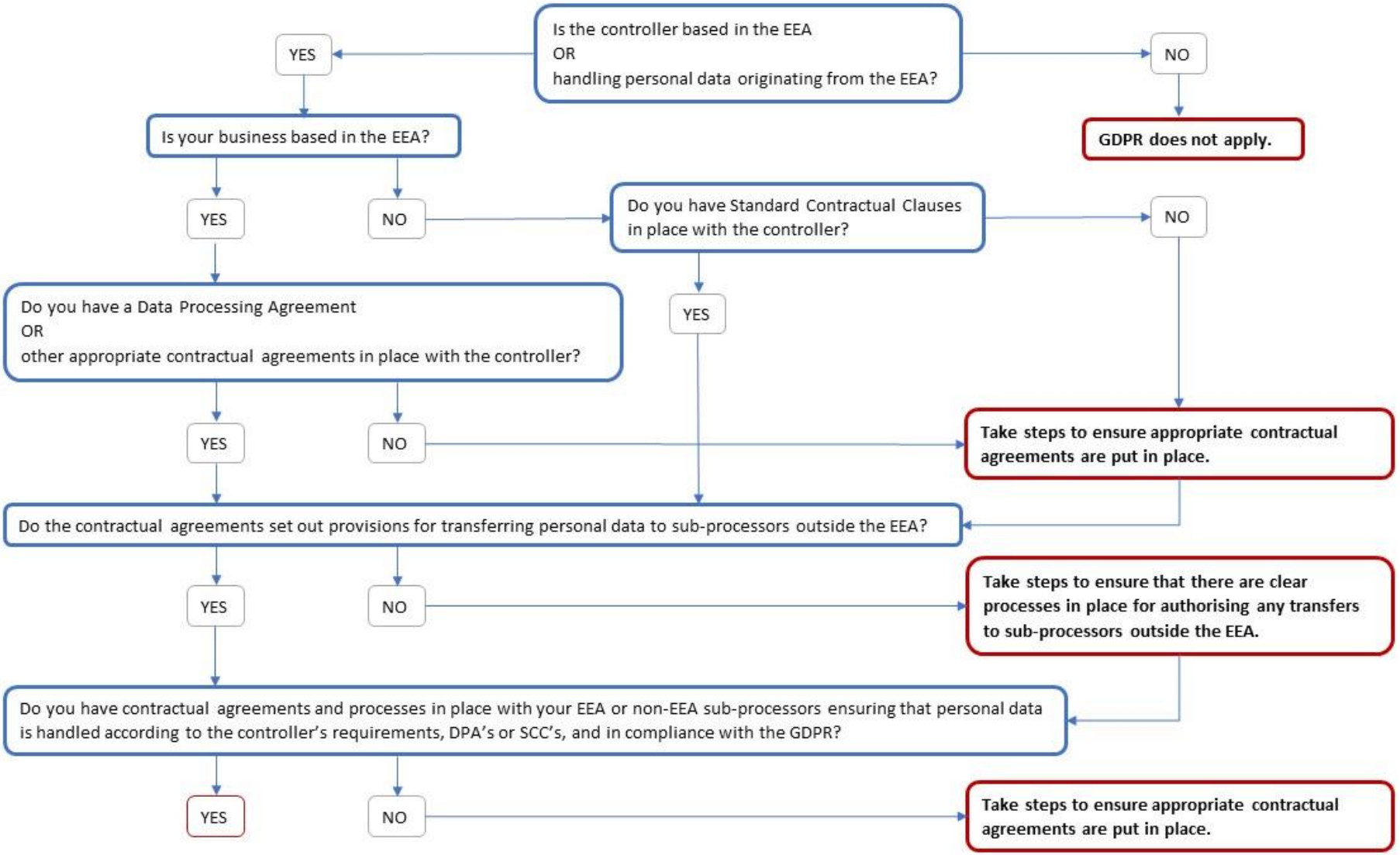
ANNEX III: Risk Assessment by Content Type

ANNEX I: Readiness Checklist

TOPIC	READINESS CHECK	✓
Awareness	Do you and your staff understand the key concepts and principles of the GDPR, and your obligations in keeping data subjects' personal data secure?	
	Do your suppliers understand the key concepts and principles of the GDPR, and their obligations in keeping data subjects' personal data secure?	
	Is the data controller aware of their obligations under the GDPR when it comes to personal data in content for translation?	
Contractual	Have you defined the roles of controller, processor and sub-processor within your translation supply chain?	
	Has the controller put in place a Data Processing Agreement?	
	If not, have you included appropriate contractual elements in your Terms & Conditions with the controller to ensure GDPR compliance?	
	Have you put in place appropriate contractual agreements with sub-processors in the EEA and in adequate countries?	
	Have you put in place Standard Contractual Clauses or other appropriate safeguards with sub-processors in third countries?	
Content risk assessment	Have you carried out a risk assessment based on content for translation and the level of risk associated with personal data in that content?	
	Have you put in place appropriate processes for handling content for translation based on the level of risk associated with personal data in that content?	
Data transfers	Have you carried out a risk assessment on data transfers?	
	Have you got the controller's authorisation to transfer data to sub-processors?	

	Have you got the controller's authorisation to transfer data to third countries?	
	Have you put in place appropriate processes for transferring content outside the EEA?	
Data retention	Have you carried out a risk assessment on data retention periods?	
	Has the controller defined appropriate data retention periods?	
	If not, have you defined appropriate data retention periods?	
	Have you put in place appropriate processes for complying with the defined data retention periods, and for ensuring that any sub-processors comply with them?	
Data security	Have you got appropriate technical and organisational safeguards in place to ensure the security of the data you process?	
	Have you ensured that any sub-processors have the appropriate technical and organisational safeguards in place to ensure the security of the data they process for you?	
Documentation	Are you keeping records of processing activities, including details of the controller, categories of processing and transfers of personal data to third countries?	
	Have you documented general descriptions of technical and organisational safety measures?	
	Have you documented your risk assessments and processes?	
Continuous improvement	Have you got processes in place to monitor compliance?	
	Are you reviewing your risk assessments and processes regularly, and taking appropriate action to improve them?	

ANNEX II: Contracts and Transfer Routes



ANNEX III: Risk Assessment by Content Type