A Brief Guide to the GDPR

Institute of
Translation
and Interpreting

Please note:
This guide was originally produced for members of the Institute of Translation and Interpreting (ITI). The information provided here is for general information purposes only and ITI assumes no legal responsibility or otherwise for omissions or errors in the contents of this guide. Always take data privacy seriously and we recommend that you seek appropriate legal advice on any specific matter.
ITI cannot guarantee the accuracy, relevance, timeliness or completeness of any information found here or on any of the external links provided in this guide.
24 May 2018

A Brief Guide to the GDPR

Contents

1. Introduction

Firstly, and above all, don't panic and don't focus on 25th May as a deadline. As the saying goes, 'Keep Calm and Carry On'.

Secondly, be aware that there is a lot of GDPR misinformation out there; including unnecessary scaremongering, conflicting advice, well-meaning but misinformed friends, and organisations hoping to make a quick buck out of the confusion. If in doubt, we recommend that you refer to the ICO website www.ico.org.uk and stick to that as your definitive source of information. As the UK's Supervisory Authority, it's the ICO that would be most likely to step in if there was a problem, so it makes sense to go along with what they say. Of course it doesn't help that their own advice can be vague, open to interpretation, and even contradictory – but their attitude is one of support, education and consultation.

They repeatedly state soothing words to the effect that if you're doing your best and taking data privacy seriously, then you have nothing to worry about (least of all £20M fines and legal action). Note that the Supervisory Authorities have some flexibility in how they apply the requirements, plus the GDPR will also sit alongside member states' national legislation. Other EU associations will be advising their members according to their own particular set of circumstances, so this is another reason to minimise confusion by sticking with the ICO.

As professionals, you all take data confidentiality in your stride, almost without a second thought. GDPR compliance will end up similar to this and you will soon wonder what all the fuss was about.

2. Background

In the UK we currently have the Data Protection Act of 1998 that already includes most of the definitions, concepts and requirements that we have in the GDPR. We can assume that it has largely been ignored given the amount of fuss over the GDPR that we see now. Anyone worried that their business is about to implode due to the GDPR, might want to consider that the Data Protection Act hasn't had much of an effect on them so far.

Note there is a new Data Protection Bill currently going through parliament that will eventually sit alongside the GDPR, plus we have other legislation out there such as the current PECR (Privacy and Electronic Communication Regulations) and its eventual replacement - a forthcoming EU ePrivacy Regulation - to be aware of too. As we have plenty of national legislation of our own, whatever the government does about EU legislation, Brexit is unlikely to have any effect on your data protection obligations.

This complex regulatory landscape recognises that personal data is a valuable commodity; it has been described as 'the new oil'. The broad aim is to put individuals rather than businesses in control of our personal data, giving us rights to know who has it and what it's used for, and empowering us to make informed decisions over what happens to it. This can't be a bad thing. You only have to look at your own email inbox and the raft of messages asking you to opt-in or read a new privacy policy to get a snapshot of how far and wide our data is used.

A Few Important Concepts

3. What is Personal Data?

- Think of it in terms of 'just about everything that could identify an individual.'

Broadly, it is any information that can be used to identify a living person. So this can include names, photographs, location data, online identifiers etc. The regulation also considers 'special categories of personal data' which is more sensitive information that is afforded greater protection "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…" (Article 9)

4. What is 'processing' personal data?

- Think of it in terms of 'doing just about anything' with personal data

"Processing means 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 combination, restriction, erasure or destruction" (Article 4 (2))

As a translator or interpreter (non-exhaustive list)

- it's the receiving, reading, translating, putting through TM, storing and returning of texts that contain personal data
- it's reading, storing, destroying or returning any reference material you are given that includes personal data
- it's making, storing and destroying notes that you have made that include personal data
- it's the written communications with clients/agencies if you use an individual's name (johnsmith@ rather than info@)
- it's keeping and using the data that you need for invoicing and record-keeping
- it's the exchange of business cards at an event (but do not overthink this)
- it's having a Christmas card list of clients/agencies (do not overthink this either)

5. What is a Controller and what is a Processor?

This is a key concept to understand because the GDPR has different provisions depending on whether you are a 'Controller' or a 'Processor' of personal data, and you'll need to know which you are when you're referring to the ICO website. Unfortunately, it's not always a black and white distinction, and this is where case law in the coming years will help define the two roles in practice.

It's also another reason why you'll see conflicting opinions as people interpret the grey areas in different ways. It's just too early for absolute certainty.

The ICO says:

- A controller determines the purposes and means of processing personal data.
- A processor is responsible for processing personal data on behalf of a controller.

If we think about personal data in a text that is sent to an agency by a corporate client, we can be confident that the client is a controller. The client knows why it wants the translation (purpose of processing) and it has decided to get an agency to do it (means of processing).

The agency is responsible for carrying out the instructions of the client and is therefore the processor. The agency sends the source text to a freelance translator. The translator is a sub-processor.

That much is fairly straightforward, however note that the GDPR also provides for Joint Controllers, and there could be an argument that the agency is also determining the means of processing by selecting the most appropriate translator. When asked about this, the ICO responded that it is a matter of legal opinion that they cannot provide.

Either way, the role of the translator/interpreter as far as doing the work is concerned in this scenario, is fairly clear to be that of a Processor. You will also have activities for which you are also the Controller, such as your admin and accounts. You need this information for your own purposes and you decide how to deal with it. But your core business activity is still that of a Processor.

Variables in this supply chain might change things. If you work for a direct client who is the data subject (say translating their birth certificate) there is an argument that you could be a Joint Controller, and/or if you sub-contract work out further, say for proofreading, you could be a Controller for that aspect of the processing which could be considered as part of your core business activity. Depending on what you do with TM files, you could be a Controller for the personal data within them.

The chances are that you will fall in and out of these scenarios depending on the nature of your work. You will have to make your own assessment of your own circumstances. Make a note of your rationale for whatever you decide. The following is going to assume you are a Processor.

What to do now and what to expect

As a Processor, any Controller that works with you, should be satisfying themselves that you will be GDPR compliant by 25th May (or that you are actively working on compliance).

They will be looking for your assurances that your processing activities are or will be within the law.

You can help demonstrate this by having a **Privacy Notice** available to them (see below).

They should supply you with a **Data Processing Agreement (DPA)** for you to sign. The DPA is a requirement of the GDPR and must include certain information. Unfortunately and unavoidably, this means that DPAs are long, and at first glance very complicated, but don't be put off. They will soon become standard procedure. The DPA provides you with a certain amount of protection because according to the GDPR, should things go wrong, as long as you have acted in accordance with the instructions of the DPA, you will be OK. Without a DPA you are considerably more exposed. However, watch out for terms relating to liability that don't appear to meet this requirement. The DPA should also specify retention periods for the data as this should be determined by the Controller. You will need to make sure that use of TMs is covered and also consider your own retention timescales – perhaps for insurance requirements. A client could include a DPA as part of other agreements with you, but it is highly unlikely that any existing Non-Disclosure Agreements (NDAs), confidentiality agreements, or other terms that you have previously agreed with clients, will contain the content required for a DPA.

For a sample DPA, see https://www.dlapiper.com/en/uk/insights/publications/2017/08/example-gdpr-ready-processor-terms/

If they're not prepared, the Controller may ask you if you have a DPA that could be used. There's no reason that you couldn't put forward your own if you have one.

6. Privacy Notice/Statement/Policy

The ICO have said that the first thing they would look for if investigating a business, is their privacy notice. This is where you set out your stall for GDPR compliance. We can expect 'ambulance chaser' companies to scour websites for Privacy Notices and to use scaremongering tactics where they find them to be non-compliant (or non-existent).

You can find out detailed information about what should be in your Privacy Notice on the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ It should include the type of personal data that you collect and process, what your processing involves, the **lawful basis/**bases for doing it, your retention period etc. The what, how, why and when of your processing. Your audience is anyone whose data you might process, so potentially clients (direct clients and agencies) the data subjects themselves. The idea is to be transparent about where personal data is used.

You can name your suppliers if you wish, but it's fine to list the type of supplier, such as 'Accountants' or 'Cloud storage provider' Although it's not yet GDPR-ready, the ICO's Privacy Notice is an interesting example to look at https://ico.org.uk/global/privacy-notice/ but there are many ways to present the information. In the interests of transparency, your Privacy Notice should be in the language(s) most easily understood by your customers.

This task seems daunting, but your privacy notice won't have as much information as the ICO, and once you get started it should get easier. Don't worry about having a perfect policy from the outset.

You can add to it as time goes by, but at least have something, even if for now it's a short statement acknowledging your responsibilities to look after personal data, confirming that you take data security seriously, and that you don't share details with anyone else beyond your processing.

You might want to include your short statement in your email signature, and you should point out that you have a privacy notice available on request (and provide a link to it on your website if you have one).

7. Lawful bases for processing

As a Processor, you do not need to worry about the lawful basis for your processing. That is the responsibility of the Controller. (Although if you think their instructions to you are illegal, you are supposed to let them know. What happens after that isn't clear…)

There are 6 lawful bases available for processing the personal data that you control. See the ICO website for comprehensive information.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

In your case, these are likely to include legal obligation (eg keeping records for tax purposes), contractual (where you have a contract with the data subject – not just any contract), and legitimate interest (broadly for operating and growing your business, but there's a lot more to it).

There is a lot of GDPR 'noise' about consent. Having the data subject's consent for processing might seem a straightforward solution, but this can cause problems if their consent is later withdrawn. It's a good idea to identify a different lawful basis than consent wherever possible.

Familiarise yourself with the lawful bases and the terms used as soon as you can, as you'll need to consider them as part of your privacy notice.

8. TM files

The GDPR was drafted in a way to encompass all businesses and processing activity, but as it stands it does not accommodate the use of TM files very well. There is no definitive answer or advice on this issue. Some thoughts to consider:

As written in the legislation, all personal data should be returned to the Controller at the end of the processing. This means that personal data contained within TM files, shouldn't be retained. As it can't be extracted, theoretically the use/retention of TM files is not permitted under the GDPR (and probably under the current Data Protection Act too)

There is a provision for when a Processor acts outside the DPA, they become a Joint Controller for that personal information. That would mean you need a lawful basis for having personal data in the TM, and the other liabilities that go with being a Controller.

The spirit of the GDPR is transparency regarding the use of personal data, so with that in mind, it could be preferable to deal with the TM question as part of the DPA.

The GDPR does not like the retention of personal data indefinitely, as it cannot be justified. This could be the case for TM files (or at least for as long as the translator was working). The indefinite

retention is solely in the interest of the translator, not the data subject. You might read about exceptions to indefinite retention for historical research etc, but it's probably too much of a stretch to think that this exemption would cover a TM file – although you might think otherwise.

It's arguable that the personal data within TM files is effectively 'scrambled' into segments, and therefore the risk of identifying anyone from the files is very low. If a data subject can't be identified, GDPR does not apply. That thinking, combined with ensuring that access to the TM files is restricted and protected by passwords, is another approach you could take. If your TM is cloud-based, ensure you have a DPA with the provider.

In due course there may be a technical solution from the TM software providers. Whether this would deal with legacy data or just new data remains to be seen.

In any event, in the interests of data privacy (if not intellectual property), the sharing of TM files should be discouraged. Check if your software has an option to share your files in the cloud, and make sure it's not enabled.

9. IT Security

Give some thought to your IT Security and the security of files that you send/transfer. Whatever you do with personal data, at least if it's protected in some way, the risk of potential harm starts to reduce.

Note that the GDPR does not require encryption of files, it calls only for 'appropriate technical measures'.

The sending of files by email is generally considered not to be secure, however your clients may continue to send files this way. Password protecting any attached files is at least a step in the right direction. File transfer services such as DropBox or We Transfer are another solution, but if you are initiating the transfer, you should check that such services are GDPR compliant, and have an agreement in place with them (or agreed terms of use).

- As a minimum, password protect files including those that you transfer to USB devices.
- Ensure your anti-virus software is updated regularly and update other software that you use as soon as possible.
- Be aware of phishing emails and other scams that could compromise your data or prevent access to your files. There are fake GDPR emails doing the rounds at the moment, so remain vigilant.

10. Place of Work

The GDPR limits the transfer of personal data to 'third countries', which are those outside the EEA, and those not deemed to provide an adequate protection to the rights of data subjects. Countries outside the EEA that ARE deemed to have adequate protections are currently Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield – a scheme for businesses).

- If you travel to a third country and do any work there (ie process personal data) you may be in breach of your DPA with your client, and in breach of the GDPR. Perhaps that's a good reason to leave your laptop at home (safely locked up and password protected, of course) when you go on holiday…
- If you are based in a third country, or need to work from there, you should discuss this with your client(s).

11. Breach

As soon as you are aware of a breach, as a Processor you should inform the Controller who will decide if the ICO should be notified.

As a Controller, you should take appropriate action. For more information and to learn what constitutes a breach, please see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

12. Registering with the ICO

Under the current Data Protection Act Controllers generally need to register with the ICO. This requirement changes slightly under the GDPR. There will be a requirement for Controllers to 'pay the data protection fee' and the concept of 'registering' will end (although there will be a register of those who have paid the fee – just to add to the confusion).

- If you have previously registered with the ICO then it's highly likely you will need to pay the data protection fee (£35/year) at renewal. The ICO will contact you about this.
- If your core business is as a Processor only, then you probably do not need to pay the fee. (Personal data that you control only for accounting and admin is disregarded).
- If you have a wider Controller role, for example because you work with a proof reader, or subcontractor(s) of any kind, or you are a Controller for your TM files or for any other reason, then chances are you do need to pay the fee.
- There is a self-assessment tool on the ICO website to help you.
- You can pay the fee voluntarily if you want to err on the side of caution and/or to be able to point to having paid the fee as evidence of taking the GDPR seriously. In any event, don't spend £35 worth of your time worrying about it.

The ICO website is overwhelmed with people trying to pay the fee. If you do decide to pay the fee, there is no need to rush. Remember nothing bad has happened because you weren't registered under the Data Protection Act, so you can probably take your time now. GDPR-wise, that time will be better spent working on your privacy notice and reviewing your IT security.

For more information, see https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf

13. Marketing

No doubt you are being bombarded with GDPR-related emails asking you to confirm your consent to receive marketing information, or to read new privacy policies. Whether these are necessary (or lawful) will depend on the particular circumstances of the sender, and your status as an individual or a company. You are not privy to all these circumstances, so we urge caution in assuming that your own marketing database must be treated in the same way. GDPR and PECR have some overlap here, and detailed guidance is available from the ICO https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/direct-marketing-checklist/

You'll need a lawful basis to send marketing information to contacts on your database. This could be the basis known as 'legitimate interests' OR 'consent'.

As a broad summary, If the recipient is a current or previous customer (a company), or you have been in negotiations regarding their custom, perhaps by providing a quote, then you can continue to market to them, assuming it's only in respect of your translation or interpreting services (not your holiday home or any unrelated product or service). They must have been advised that they could opt out of such communications, and every future communication must also make it easy for them to opt out. This scenario allows marketing as a 'legitimate interest'. It's also referred to as the 'soft opt-in' under PECR. Ideally you need to inform these contacts that you have an updated privacy policy and remind them that they can opt out of marketing communications at any time. Note this isn't the same as withdrawing consent, because you are not processing data on the basis of their consent in the first place. Given the influx of GDPR emails that try everybody's patience, you might decide to wait before sending your privacy policy – at least until you're ready to send your next mailshot. You may also decide that you can continue marketing to companies as a legitimate interest of your business (but see ICO guidance for details).

If this soft opt-in doesn't apply, and you're email marketing to private individuals, sole traders or partnerships and the communication is unsolicited, then you'll need consent. GDPR introduces a higher standard of consent than under the Data Protection Act, such as not using pre-ticked boxes, but requiring a clear and affirmative action on the part of the data subject. If you need fresh consent because you don't yet have a GDPR standard of consent, then you need to get this before 25 May – hence the inbox influx. If you didn't have consent in the first place, you can't lawfully email to request consent. If you're relying on consent as your lawful basis, then you cannot lawfully send marketing information to anyone where you don't have the GDPR standard of consent – so they should be deleted from your database.

If you've asked for consent because everyone else did, and now realise that you didn't have to, you have until 25 May to change your lawful basis.

Please see the ICO Guidance for more information as we cannot cover every scenario here.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

14. Communications within groups

If you run a group, you will be a controller in respect of the personal data of your group members. This means that you need to establish the lawful basis for using their data. In this scenario, it's likely that 'Legitimate Interests' or 'Consent' would be possible lawful grounds. As consent can be more of a headache to deal with, in terms of getting it right and dealing with any subsequent withdrawal of consent, 'Legitimate Interests' should probably be relied on here (subject to checking ICO detailed guidance). Incidentally, if you are Admin for a Facebook Group, as long as the personal data is contained within Facebook, the processing is subject to Facebook's policies and terms.

15. Getting it wrong

Remember the ICO does not have a team of enforcers sweeping the country like TV license detector vans. In fact the ICO's current enforcement team consists of just 60 people. They have bigger fish to fry than individual translators and interpreters. As long as you are not playing fast and loose with personal data, you can be fairly certain that you will never come to their attention. When you look at the relative risks involved, perhaps it is not worth tying yourself in knots over the minutiae of the GDPR. If you do your best (and remember the process is ongoing, not just a snapshot), if you take the trouble to be GDPR-aware, and if you document all the decisions that you make, then you should be fine.

16. Getting it right

This document has only scratched the surface of the GDPR. To methodically work through your compliance, use the free resources on the ICO website. Their advice is being updated all the time. The '12-steps' guide is very user-friendly, and we recommend you take a look. Beyond that there's a more comprehensive self-assessment toolkit. If you are a Controller for 'special categories' of personal data, pay close attention to the additional requirements for this.

See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Good luck!

