



How to Prepare for the GDPR

This is a checklist for the EU Data Protection Regulation (GDPR).

Introduction

This document is a “how to” guide, for website admins. It lists the steps that I think you need to take to support the GDPR.

It also includes two audits, with data for Fresh Relevance: a Data Protection Impact Assessment (DPIA) and a Legitimate Interests Assessment (LIA). Use these as worked examples of what’s involved, or for reference if you are acting as a Data Controller and we’re your Data Processor.

It is written by Peter Austin, Data Protection Officer, Chief Innovation Officer and Co-Founder.

The content of this document will change to reflect changing official advice about the GDPR. This version is dated 4/10/2017. You can find the latest version here: <https://www.freshrelevance.com/contact/legal>

What is the GDPR?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a new regulation that becomes enforceable from 25 May 2018. It strengthens and unifies data protection for all individuals in the European Union and gives them new rights, such as data portability. It also restricts the export of personal data outside the EU.

Text of the GDPR:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

References in square brackets refer to this, for example [Preamble 22] means item 22 in the preamble.

UK Data Protection Bill 2017, published on 14 September 2017.

<https://www.gov.uk/government/collections/data-protection-bill-2017>

Draft version of the bill which will implement the GDPR in the UK

You should also read the UK Information Commissioner’s Office Website and follow their blog:

<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/>

<https://iconewsblog.org.uk/>

Some Definitions

- European Union = The Union = EU = most of Europe
- Natural person = individual = person = data subject
- Legal person = company or business
- Data Controller = business which owns personal data, e.g. an ecommerce site
- Data Processor = subcontractor to the Data Controller, e.g. a marketing technology provider

Is my Business affected by the GDPR?

Your activities are affected by the GDPR if all the following apply (see Appendix 1):

1. You are **not** just a private individual, performing a purely personal or household activity.
2. You are processing data about people, not just companies or businesses.
3. The data is identified or identifiable. Genuinely anonymous data is irrelevant.
4. You are based in the EU, or you are based elsewhere but some of the people whose data you process are in the EU. Note that the test is “in the Union”, not “resident in the Union”, so it seems that you are caught by the GDPR if people for whom you hold data, possibly collected at a time when they were outside the EU, are currently visiting the EU on holiday.

The GDPR applies to ‘controllers’ and ‘processors’. the controller (for example the owner of an ecommerce website) says how and why personal data is processed and the processor (for example the operator of some technology used by the website) acts on the controller’s behalf.

- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.
- If you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. See: <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>

Reference: [Obligations of controllers and processors under the GDPR – The Law Society.](#)

What if a Data Processor subcontracts work to another Data Processor, does this make them a Data Controller too? No, it doesn't. They remain a data processor and the GDPR calls the new one "another data processor". There is usually just one Data Controller, the original one, and "the data processor cannot choose to enter into sub-processing arrangements without [their] approval". Basically, each Data Processor needs to tell the Data Controller of all the other Data Processors that they plan to use (which could be a lot) and get prior permission, which could be pretty ugly, but data processing agreements can grant outline permission in advance to get around this. Reference:

https://ico.org.uk/media/for-organisations/documents/1585/outsourcing_guide_for_smes.pdf

Checklist to Prepare for the GDPR

Did you just discover that you are affected by the GDPR? [Start by reading my blog about GDPR Myths](#), which corrects a lot of the mistakes out there.

Then follow this checklist:

1. Do you hold data about vulnerable people or children [preamble 75], or deal with high value data where loss could lead to discrimination, identity theft or fraud, financial loss, damage to the reputation, or any other significant economic or social disadvantage? [preamble 75-77]
 - a. Don't just rely on a standard checklist – you need expert advice.

2. Appoint a GDPR Data Protection Officer

- a. Appoint a GDPR data protection officer [Article 39]. Read the reference for a description of the role. They can be responsible for everything from record keeping to acting the contact person for data subjects (e.g. customers), and for monitoring compliance.
- b. Put contact details for your GDPR data protection officer on your website, so data subjects can easily contact them to enforce their new rights.
- c. If you are a Data Controller, you may have data processors (tech providers and subcontractors) – all organizations that handle identified or identifiable personal data related to your business, e.g. your ESP and social networks. Collect contact details of their GDPR data protection officers, and details of data processors they subcontract to.
- d. If you are a Data Processor collect contact details of your Data Controller's GDPR data protection officer.
- e. Ensure decision makers and key people in your organization are aware of the GDPR
- f. The GDPR is not limited to shoppers and customers, or to digital data. It applies to all identified or identifiable individuals whose personal data you hold, including your staff and including data in manual filing systems [preamble 15]. This is a reminder to check all parts of your business for compliance, for example personnel not just ecommerce.
- g. You will eventually have to update all your processing/subprocessing contracts to comply with the GDPR. I expect that standard short contracts, designed to insert the extra GDPR terms into existing contracts, will become available in Spring 2018. Further discussion is beyond the scope of this document.

See the UK ICO Outsourcing Guide for SMEs:

https://ico.org.uk/media/for-organisations/documents/1585/outsourcing_guide_for_smes.pdf

3. Perform a Data Protection Impact Assessment (DPIA) - see details later
 - a. If you have never carried out a Data Protection Impact Assessment, or not recently, do so now. What data are you holding? For how long? For what purpose? Can you reduce it? Is there a high risk, so you need to contact your Supervisor Authority? [preamble 89-90]
 - b. If any of your data processors is responsible for data about your data subjects, request and check their Data Protection Impact Assessment.
4. Only Collect and Keep the Data You Need, based on the DPIA
 - a. Stop collecting unnecessary data.
 - b. Delete aged data when it's no longer needed.
 - c. When some staff do not need to see personal data, then stop them from seeing it. By technological measures where possible, supplemented by training and changing your business processes.
 - d. If you are a Data Controller, confirm that your Data Processors (technology providers and subcontractors – and their subcontractors) have done the above (a-c).
 - e. If you are a Data Controller, then update your privacy notice(s) to report the data that you and your data processors are collecting and why. Keep it very simple. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, using clear and plain language [preamble 39].
 - f. If you are a Data Processor, confirm that your Data Controller has done the above (e)

5. Is Your Personal Data Transferred to a Third Country?
 - a. Remember that personal data is only affected by the GDPR if it is “identified or identifiable” [preamble 26]. Anonymous data can be transferred without restriction.
 - b. List of countries where you and your Data Processors can transfer personal data of people in the EU to:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
6. Perform a Consent and Legitimate Interests Assessment (LIA) - see details later
 - a. The GDPR has several grounds for using personal data, including consent and legitimate interest. [Article 6] If you can show that you have a sufficient legitimate interest in using personal data for e.g. marketing, then this is probably better than asking consent. You do a LIA to test this.
 - b. If any of your Data Processors handles identified or identifiable personal data on your behalf, request their LIA or else you need to do a LIA for them. Use it to check whether you need to ask consent from data subjects for any of their processing activities.
 - c. The GDPR is not the only reason for getting consent – for example there are laws in several countries to prevent spam email, such as CASL in Canada. Check whether there are non-GDPR reasons to ask your data subjects for consent.
7. On your Website and based on the LIA, Ask for any Necessary Consent
 - a. Consent to use personal data should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as ... ticking a box when visiting an internet website [preamble 32]
 - b. Draft consent guidance from the UK ICO:
<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>

8. Prepare for the New GDPR Individuals Rights

- a. The GDPR includes eight Individuals' rights. For details see <https://ico.org.uk/for-organizations/data-protection-reform/overview-of-the-gdpr/individuals-rights/>
 - i. The right to be informed
 - ii. The right of access
 - iii. The right to rectification
 - iv. The right to erasure
 - v. The right to restrict processing
 - vi. The right to data portability
 - vii. The right to object
 - viii. Rights in relation to automated decision making and profiling.
- b. Decide how to implement the Individuals' rights and write eight scripts, one for each of the above rights, for you or your staff to follow whenever a data subject requests these.
- c. If any of your Data Processor(s) handles identified or identifiable personal data on your behalf, you will have to include them in the actions taken whenever a data subject requests their rights. So ask your Data Processor(s) how to do this; get instructions from them if appropriate; and add their instructions to your scripts.

9. Decide how to Identify Individuals who request their rights.

- a. Suppose you have a customer called Pete-and-Linh. Someone phones your support line, saying he is "Peter Austin", claims he is the same person as your customer Pete-and-Linh, and he wants to enforce his "right to data portability" by you sending a copy of all "his" data immediately. How do you know that he gave you his correct identity and that he is the same person as your customer. Or is he an identity thief?

- b. You need a process to confirm the identify of people who contact you, asking to enforce their new rights, without making life too hard for honest citizens, or enabling identity thieves. Bear in mind that this is not only about customers, but anyone in the EU for whom you hold identifiable personal data, e.g. because they visited your website or used your app. NB consider that you may not always have a credit card number or email address for them and you can't ask this information unnecessarily, because the GDPR requires you to only collect data that is necessary (data minimization) [preamble 5.1.c]
 - c. This basically comes down to deciding: what information do you have that only the genuine data subject will know, that you can use to check they are legitimate.
10. Create a Data Breach Response Plan.
- a. The GDPR makes you react quickly to data breaches: "the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay". [preamble 85]
 - b. Create a Data Breach Response Plan, in advance, and ideally organize a simulation, so the people involved can play through it. Although 72 hours may seem ample time, it really isn't. Consider that you will need to consult with third parties such as your Data Processor(s) and that hackers are known to attack on weekends and public holidays.

Here's the ICO's alternative checklist, "Preparing for the General Data Protection Regulation"

<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>

I also like this: Unlocking the EU General Data Protection Regulation - A practical handbook on the EU's new data protection law – White & Case

<https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation>

Appendix 1: Is my Business Affected by the GDPR?

The tests for whether your business is affected by the GDPR are based on the following references in:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

References in square brackets refer to this, for example [preamble 14].

- The GDPR applies to “natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons” [preamble 14]
- The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. [preamble 15]
- 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. [preamble 18]
- Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. [preamble 22]
- the processing of personal data of data subjects who are **in the Union** by a controller or a processor not established in the Union should be subject to this Regulation. ... [Or if it is] apparent that the controller envisages offering goods or services to data subjects in the Union. [preamble 23]
- The GDPR does “not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person ... This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes” [preamble 26]

NB the bold text “**in the Union**” from [preamble 23], which means in the European Union and a handful of adjacent countries such as Switzerland. This I think is the crux of the whole document for martech vendors such as advertising networks. The test is “in the Union”, not “resident in the Union”, so it seems to me that you are caught by the GDPR if any people for whom you hold identified or identifiable personal data, even if collected when they were outside the EU, are currently visiting the EU on holiday.

Appendix 2: Example Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment is needed when you first comply with the GDPR, or whenever you significantly change processing.

The following DPIA is a worked example for Fresh Relevance Ltd. To do an audit for your business, delete the Answer column and answer the questions for yourself.

The content is based on the official GDPR Text, page 164 section 3, at the following URL. As usual, references in square brackets refer to this PDF, so e.g. [p164 3] means page 164 section 3.

<http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/en/pdf>

A: Data Protection Impact Assessment? [preamble 35]		
Question	Answer	Help
N/A	N/A	Consider each of your processing operations in turn, e.g. one might be personalizing Web pages, and another sending marketing emails...
1 Describe the data processing operation	Scrape shopping data; personalize marketing; trigger msgs; research.	
2. For this data processing operation: What personal data are you holding? How long?	Details of products browsed, carted and purchased; marketing scheduled and seen. Optional first+last name and email.	Only include identified or identifiable personal data. "The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". [preamble 35.1]

3. Does your data collection meet GDPR Principles?	Yes	<p>Personal data must be. Look at the reference for the full version: [preamble 5]</p> <ul style="list-style-type: none"> a) processed lawfully, fairly and in a transparent manner b) collected for specified, explicit and legitimate purposes c) adequate, relevant and limited to what is necessary ('data minimization') d) accurate and, where necessary, kept up to date e) kept in a form which permits identification of data subjects for no longer than is necessary
4. Describe any changes to meet GDPR Principles.	None	
5. Only analyze the processing operation further if it could be a high risk to data subjects. Otherwise skip the remaining questions about it.	No (It's not a high risk so skip the remaining questions.)	Could it result in a high risk to the rights and freedoms of data subjects? If yes, try to make changes to the processing operation so the answer is no. If no, you do not need to continue the DPIA for this processing operation, so skip the remaining questions. Read [preamble 35.1].
B: Data Protection Impact Assessment, Questions if there could be a High Risk [p164 35]		
Question	Question	Question
6. Describe the data processing operation		Make a systematic description of the envisaged processing operations and the purposes of the processing [Article 7.a]
7. What are the Legitimate Interest of the controller?		Describe the legitimate interest of the controller [Article 7.a]
8. Why is the operation		Assess the necessity and proportionality of the processing operations in relation

necessary?		to the purposes [Article 7.b]
9. What are the risks to the rights and freedoms of data subjects		Assess the risks to the rights and freedoms of data subjects [Article 7.c]
10. How can the risks be reduced?		Describe the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data [Article 7.d]
11. Does it comply with approved codes of conduct?		Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. [Article 8]
12. Do you need to seek the views of data subjects?		Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. [Article 9]
13. Based on the above, answers, will it result in a high risk to the rights and freedoms of data subjects?		The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36.1]
14. If the previous answer is "yes", what further		

<p>measures will you take to mitigate the risk?</p>		
<p>16. If the risk is still high, contact your supervisory authority (ICO in the UK).</p>		<p>When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:</p> <ul style="list-style-type: none"> a. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings [Article 36]; b. the purposes and means of the intended processing; c. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation; d. where applicable, the contact details of the data protection officer; e. the data protection impact assessment provided for in Article 35; and <p>any other information requested by the supervisory authority. [Article 36]</p>

Appendix 3: Example Consent and Legitimate Interests Assessments (LIA)

There are examples on the [Fresh Relevance legal page](#).