Guide

UK GDPR Documentation

measured collective

An overview of the documents mentioned in UK GDPR. What they are, the legal basis for preparing them and who should prepare them.

Disclaimer

Although we go to great lengths to deliver accurate and useful content. Please be aware that advice from us cannot be considered a substitute for professional legal advice, nor do they create an attorney-client relationship. Regulations can change at short notice. We advise you to seek your own professional legal advice.

Content & Licensing

We've gone to great lengths to source our base content and knowledge from reputable sources. Where possible we have prioritised court rulings and guidance issued directly from legislators, for example from the European Commission in relation to GDPR. We have supplemented this with guidance from the national regulators who enforce these regulations. Our aim is to give you content that is up-to-date, factual and useful.

Core documentation required

The document	Legal basis	Who should prepare this documentation?	About the documentation	Done or N/A?
Designation of a data protection officer (DPO)	Art. 37 UK GDPR	All companies that need to appoint a data protection officer	The appointment of the DPO should be kept in writing. It is also a good idea to document the tasks of the DPO as part of the written agreement. The DPO designation should be completed internally. Remember you should also register the appointment with the ICO.	
Legitimate Interests Assessment (LIA) - Weighing of interests	Art. 6 (1)(f) UK GDPR	Data Controller if you are relying on Legitimate Interests for any processing activities.	An LIA is a type of light-touch risk assessment based on the specific context and circumstances of the processing. Conducting a Legitimate Interest Assessment (LIA) helps you ensure that you can rely on the legitimate interests as a lawful basis of processing. You should perform it before you start processing the data and it should cover the following parts: Purpose test (Is there a legitimate interest behind the processing?). Necessity test (Is the processing necessary for that purpose?). Balancing test (Is the legitimate interest overridden by the individual's interests, rights or freedoms?)	

Data retention and deletion policy	Art. 17 UK GDPR	Any controller who carries out processing activities	An internal document that covers each category of personal data. Covers the conditions under which data is retained, how long it is retained for and under which conditions it is deleted (for example, 3 months after the end of any potential legal claims, no longer than 4 years). It is also good practice to link to any data deletion processes, to ensure that your “retention policies” can be actioned effectively.	
Implementation of appropriate technical and organisational measures (TOMs)	Art. 24 (1), Art. 25, Art. 32 UK GDPR	Every company (both the controller and the data processor)	One-time effort: a general description of the technical and organisational measures in place constitutes part of the Directory of Processing Activities, Art. 30 (1)(g) and Art. 30 (2)(g) UK GDPR.	
Data processing agreements	Art. 28 (3), (4) UK GDPR	Any controller who engages data processors, as well as data processors who engage sub-processors.	A data processing agreement (DPA) is a legally binding document between the controller and the processor covering details of the processing – such as its scope and purpose, and the protections it affords to personal data.	

Proof of data processing instructions received from the controller, and the obligation of the employees to maintain confidentiality	Art. Art. 28 (3)(b), 29, 32 (4) UK GDPR	Companies working with controllers as data processors, data processors	Documentation of the instructions given by the controller, for each instruction given. Documentation of employees obligation to to confidentiality.	
Records of Processing Activities	Art. 30 (1)(a – g) and (2)(a –d) UK GDPR	All companies in which data are processed (controllers and data processors). There is no obligation for companies with less than 250 employees to provide this, unless: • The data processing involves a risk to the rights and freedoms of the data subjects. • The data processing takes place on a regular basis. • The data processing covers special categories of data in accordance with Art. 9 UK GDPR (for example, health data, information on religion or political opinions) or data relating to criminal convictions and offences as defined in Art. 10 UK GDPR.	At a minimum you will want to answer the following questions in your records of processing: • Why do you use personal data? • Who do you hold information about? • What information do you hold about them? • Who do you share it with? • How long do you hold it for? • How do you keep it safe?	

Joint controller agreement	Art. 26 UK GDPR	Companies that, as joint controllers, determine the purposes and means of processing.	One-time documentation effort per legal entity. This should document the distribution of responsibilities amongst the data controllers in processing the data.	
D.P.I.A (Data protection impact assessment)	Art. 35 UK GDPR	This should be carried out by companies that process data in such a way that the processing is likely to result in a high risk to the rights and freedoms of natural persons due to the nature, scope, circumstances, and purposes of the processing.	This should contain, at a minimum: Description of planned processing operations and their purposes, including the legitimate interests pursued by the data controller, where appropriate. Assessment of the necessity and proportionality of the processing operations regarding the purpose. Assessment of the risks to the rights and freedoms of data subjects. Remedial action to deal with the risks.	

Data transfers to third countries (restricted transfers)

The document	Legal basis	Who should prepare this documentation?	About the documentation	Done or N/A?
Data transfers to third countries, documenting adequate safeguards and assessing the circumstances of data transfers to third countries.	Art. 30 (1)(e), (2)(c), Art. 49 UK GDPR	The controller companies that transfer data to third countries (outside the EU/EEA) (e.g., through contract processors), or contract processors themselves.	Can be included as part of your Directory of Processing Activities. SCCs and IDTAs should be documented as part of this process.	
Details of appointment of an EU representative.	Art. 6 (1)(f) UK GDPR	All controllers or processors not established in the EU/EEA (for example no office or legal company structure within the EEA) who process the personal data of EU/EEA citizens regularly and/or at scale.	Should be prepared at the point of appointment. You may wish to update other documents such as publicly available privacy policy information with these details at the same time.	
Proof of the existence of binding internal data protection rules - binding corporate rules (BCR)	Art. 46 (1), (2)(b), Art. 47 UK GDPR	Controller companies that operate across borders and wish to transfer data between individual members of the group of companies using BCRs.	Must be approved by competent data protection authorities.	

If a data breach occurs

The document	Legal basis	Who should prepare this documentation?	About the documentation	Done or N/A?
Documentation of personal data breaches	Art. 33 (1), (4), (5) UK GDPR	Controller companies that have suffered a data breach..	The documentation must take place independently of the notification to the supervisory authority, i.e., even in the case of failure to notify, the breach must be documented with the associated facts, effects, and remedial actions taken.	
Proof of notification of data subjects in the event of a personal data breach.	Art. 34 UK GDPR	Controllers in the event of data breaches that pose a high risk for the data subjects.	The need to document this is not specifically mentioned in Art. 34 UK GDPR. It is however advisable to do so, because the ICO may have to assess whether either a) the data breach requires data subjects to be notified, or b) an exception applies, and there is no requirement to notify. You should be able to document your reasoning and document how data subjects were informed if applicable. And what was said to them.	

Documents likely to be required in the event of inspection by the supervisory authority

The document	Legal basis	Who should prepare this documentation?	About the documentation	Done or N/A?
Proof of consent	Art. 7 (1), Art. 9 (2)(a) UK GDPR	Every company that processes personal data and relies on the “consent” legal basis for any processing tasks. No explicit documentation requirements in law yet documentation is recommended, as the controller bears the burden of proof for the existence of a valid consent in cases of doubt.	Electronic mechanisms will be easier to maintain, many systems can be set to record this information automatically, for example your CRM or email marketing software. At a minimum you will want to document the time and date of consent and exactly what was consented to (for example the text that accompanied the consent option).	
Proof of compliance with the rights of the data subjects	Art. 15 UK GDPR All companies, e.g., to demonstrate that the notifications made in accordance with Art. 15 to 22 UK GDPR have been complied with.	All companies that process personal data.	Document requests to exercise rights and the responses made. Document any cases where a request was deemed to be “manifestly unfounded and excessive”.	

Documents likely to be required in the event of inspection by the supervisory authority

Proof of compliance with the information requirements	Art. 12, 13, 14 UK GDPR	All companies that process personal data.	The UK GDPR does set out specifically how information requirements should be met. The ICO's guidance does suggest that all organisations prepare appropriate privacy notices and consider a layered approach to deliver information about data processing to data subjects. The ICO may request evidence of the information you have provided to data subject and how it was delivered as part of an investigation.	
Proof of the right to object	Art. 21 UK GDPR	The data controller and processor shall provide the necessary information to the data subjects before collecting and processing their personal data.	No specific documentation requirements set. However in the event of inspection by the supervisory authority, controllers must be able to prove that the data subjects have been advised of the right to objection.	

The problem with poor compliance

Fines

Non-compliance with data privacy laws like UK GDPR can be costly. Under Art. 83(5) of UK GDPR, a fine can be issued of up to 17.5 million pounds sterling or up to 4% of total global turnover whichever is higher.

Investigations

There's no greater buzzkill than a regulatory authority like the ICO turning up to your door to audit your processes, or in response to complaints.

Ethical challenges

Respecting the right of your customers and employees to privacy is the right thing to do. We can learn how to use data responsibly whilst still getting results.

Criminal liability

It's not just the company as a legal entity that can get into trouble. Individuals within the company can find themselves personally liable to be prosecuted for negligence under the Data Protection Act 2018 whether they committed the offence themselves, or they were negligent in a supervisory role.

Reputation damage

It's hard for customers and prospective employees to trust your brand when the first thing they find about you in Google is news about your latest data breach. And if you end up moving on to a new role, you'll need to be prepared for some awkward interview questions.

Losing out on investment

Investors can include data privacy law compliance as part of their due-dil, or as a bargaining chip. After all, how much is your business really worth if the customers on your database aren't even legally contactable?

Failing supplier due-dil

Established brands and public sector organisations often include data privacy law compliance as part of their procurement due-dil. If you can't complete the paperwork, you may be in breach of contract and therefore they can't be your customer.