Steps to General Data Protection Regulation (GDPR)

This guide has been provided free of charge and for guidance only. It does not constitute as a legal document or compliance advice.

Whilst LS Consultancy has made every effort to ensure that the material contained in this template is relevant and accurate, the template is only available for public viewing and use on the basis that LS Consultancy disclaim all liability to the fullest extent permitted by English Law for any loss or damage arising out of the use of this document or for any reliance by users upon its contents

Steps to General Data Protection Regulation (GDPR)

Your steps to GDPR

Understanding the regulation Initial training and awareness – aimed at firms which need to improve their understanding of GDPR. In our training and discussion session we'll provide you with an overview of the requirements and obligations of GDPR.

Output from this session will be a high level action plan identifying the key stages in implementation.

Mapping your data In order to identify the specifics of what you need to do to comply with GDPR, you'll first need to map your data. Using the ICO template (**https://ico.org.uk/media/for-organisations/documents/2172937/gdprdocumentation-controller-template.xlsx**) we will provide advice and support so you can answer key questions such as:

- What data do you gather, hold and process?
- How much is special categories of data (formerly 'sensitive data')?
- Who accesses it and in what locations?
- Where and how is it held?
- What do you use it for?
- Where did it come from and what permissions do you have to use it?
- How recent is it and how accurate?

GDPR readiness/gap analysis.

Once your data is mapped we will work through a readiness/gap analysis with you. This is a detailed, operational analysis of your firm's readiness to comply with the requirements and obligations of the GDPR. The analysis flags gaps and helps drive an action plan so you can target key risks and identify next steps; this process will also help you to assess what resources you may need to address any issues.

Advice, support and guidance

Our support includes access to a GDPR specialist to provide help and advice across the project from completing the data mapping through to creating your project plan and implementing actions. Just us the tools below;

- DPA Policy plus supporting processes and registers for each of the ....following: - Right of access - Right to rectification - Right to erasure - Right to restriction of processing - Right to object

- What To Include in marketing consent?

- Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

i. the name of your organisation;
ii. the name of any third party controllers who will rely on the consent;
iii. why you want the data; what you will do with it;
iv. and that individuals can withdraw consent at any time.

You can use: **A layered approach** – short notices containing key privacy information that have additional layers of more detailed information.

Dashboards

Preference management tools that inform people how you use their data and allow them to manage what happens with it.

Just-in-time notices
Relevant and focused privacy information delivered at the time you collect individual pieces of information about people.

Icons

Small, meaningful, symbols that indicate the existence of a particular type of data processing. Mobile and smart device functionalities – including pop-ups, voice alerts and mobile device gestures.

How to Provide Privacy Information

There are a number of techniques you can use to provide people with privacy information.

Purposes for Processing

You must be clear about what your purposes for processing are from the start. You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.

Remember: You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

So you should identify the minimum amount of personal data you need to fulfil your purpose.

You should hold that much information, but no more.

This is the first of three principles about data standards, along with accuracy and storage limitation. The accountability principle means that you need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

Also bear in mind that the GDPR says individuals have the right to complete any incomplete data which is inadequate for your purpose, under the right to rectification.

They also have right to get you to delete any data that is not necessary for your purpose, under the right to erasure (right to be forgotten).

Accuracy Principle

The accuracy principle is very similar to the fourth principle of the 1998 Act, with a couple of differences:

1. The GDPR principle includes a clearer proactive obligation to take reasonable steps to delete or correct inaccurate personal data.

2. The GDPR does not explicitly distinguish between personal data that you create and personal data that someone else provides.

However, the ICO does not consider that this requires a major change in approach. The main difference in practice is that individuals have a stronger right to have inaccurate personal data corrected under the right to rectification.

The Storage Limitation Principle

The storage limitation principle is broadly similar to the fifth principle (retention) of the 1998 Act. The key point remains that you must not keep data for longer than you need it.

The Storage Limitation Principle The storage limitation principle is broadly similar to the fifth principle (retention) of the 1998 Act. The key point remains that you must not keep data for longer than you need it.

Although there is no underlying change, the GDPR principle does highlight that you can keep anonymised data for as long as you want. In other words, you can either delete or anonymise the personal data once you no longer need it.

Instead of an exemption for research purposes, the GDPR principle specifically says that you can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes (and you have appropriate safeguards).

New documentation provisions mean that you must now have a policy setting standard retention periods where possible. There are also clear links to the new right to erasure (right to be forgotten). In practice, this means you must now review whether you still need to keep personal data if an individual asks you to delete it.

Pre and post-implementation assessment

If you feel your business is there or thereabouts, but you would value an independent view, we will conduct a verification visit to check that the processes you have in place are sufficient to meet the requirements and obligations of GDPR. This also gives you the chance to raise any issues you may have and get a specialist view.

On a more ongoing basis, we will be offering six monthly and twelve monthly post-implementation visits to evaluate how well controls and processes are working in practice and to assess future plans and developments where these might be impacted by GDPR.

Training Senior staff

We can provide specific training for decision makers and those with oversight and operational control to provide clarity about what responsibilities look like for senior staff and how these should be allocated and managed.

Operational staff

This training is aimed at those staff whose day to day activities are affected by GDPR, looking at the impact of the regulation from a more role-specific, activity-orientated perspective.

Bespoke training

Training tailored to the specific requirements of your business – including tailoring training for operational staff to reflect the firm's own GDPR processes.

Provision of an outsourced service Whether you require support with the function of the Data Protection Officer (DPO) or you simply need access to an external resource to support your business we can provide advice and assistance.