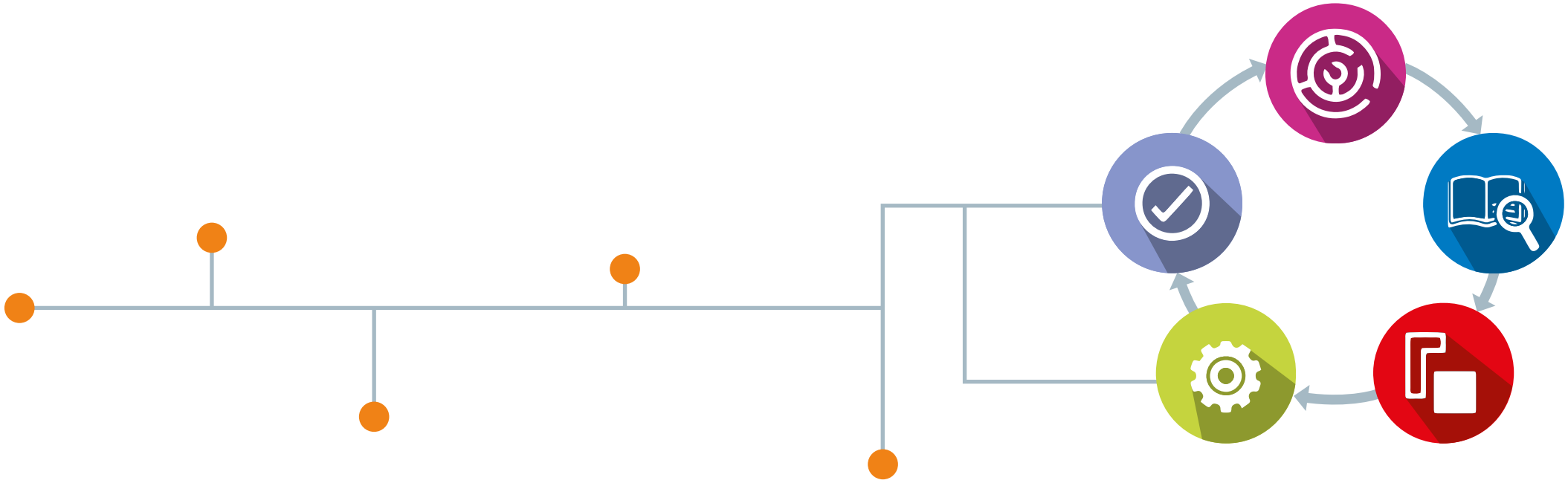
Five-step approach to General Data Protection Regulation (GDPR) compliance




1. Mapping data flows
2. Audit
3. Gap analysis
4. Implementation
5. Monitoring
The GDPR is a complex subject with many people struggling to understand the myriad of information available and how it applies to their organisation.
To help you ensure your business is GDPR compliant, Cripps has designed a simple five-step plan to guide you through the key considerations and how we can support you. Our team can help you through the entire journey or assist you at different stages depending on your needs.

1 Mapping data flows

Key considerations

How data flows into, around and out of your organisation

The first stage is focused on compiling an accurate and comprehensive record of the personal data your business uses. You need to understand what personal data you hold, the types of individuals you hold data on, and how the data comes in, moves around and ultimately goes out of the business.

To make the mapping exercise more manageable, break data down into classes of individual and types of data you hold on them. Then for each of those categories consider how you collect it (IN), what you use it for and where you store it (AROUND) and how it leaves the business (OUT).

Internal engagement

This is a detailed process which needs input across the business. Involvement from your HR, finance, marketing and IT teams will be essential. All areas of your business will handle personal data in some form, and ensuring that all of them are included in the process will help ensure that nothing is missed.

How Cripps can help

From our experience of working with several large organisations on their GDPR strategy, we can advise you on how to structure your approach and what questions you need to ask to carry out a comprehensive data mapping exercise. For example, have you considered how you will identify what is being kept on local drives, in hard copy or on mobile devices?

2 Audit

Key considerations

Reasons for using personal data

All your uses of personal data must be justified by a lawful basis. This step requires you to record for each use of each type of data, what that basis is.

Consent isn't the only basis for using personal data, but where you are relying on it, you need to examine how that consent is obtained and recorded when data comes in.

Not only does this help ensure your data processing activities are lawful, but the record of your reasons helps demonstrate compliance and will be necessary to complete your external and internal privacy notices (these provide individuals with certain information about how you are using their data).

Internal policies and procedures

To ensure that the movement and use of data around your business is compliant, you need to consider what internal policies and procedures you have in place. Retention policies (dictating how long each type of data is held) should apply to all data, and certain information may need permissions-based access and encryption protocols for greater security. If you transfer data between group companies, you also need to consider what rules or policies (including Binding Corporate Rules) apply.

Status

You need to understand your status as a data controller (an organisation which determines the purpose and means by which data is used) or a data processor (an organisation which simply carries out processing on the instructions of a controller) as this will affect your responsibility in terms of GDPR compliance.

External data sharing

You will need to assess whether data is being shared externally and if so, agreements should be in place whenever data goes out of the business, whether that's to service providers or where you're sharing data with other controllers. You'll also need to consider what privacy notices apply to that data, and how they're made available (or, if they're not, how you would make them available).

Regulation

Depending on your industry, there may be additional regulatory requirements around your use and storage of data. These need to be considered alongside your data protection obligations.

Location

This applies at all levels. You will need to assess where data is stored (for instance, on cloud servers, local machines and mobile devices) as well as whether individuals, service providers, or parts of your business are located outside the European Economic Area.

How Cripps can help

We can help you cut through the jargon and understand and interpret all the guidance that has been issued by the ICO. In understanding the regulatory requirements, you can then conduct an audit of the documented policies, procedures and protocols you currently have in place around your data to understand the level of risk in your business.

3 Gap analysis

Key considerations

Risk review

Once you have conducted your data mapping exercise and audit, you will need to understand any key areas of risk for your business, the various degrees of risk and how you are going to tackle them.

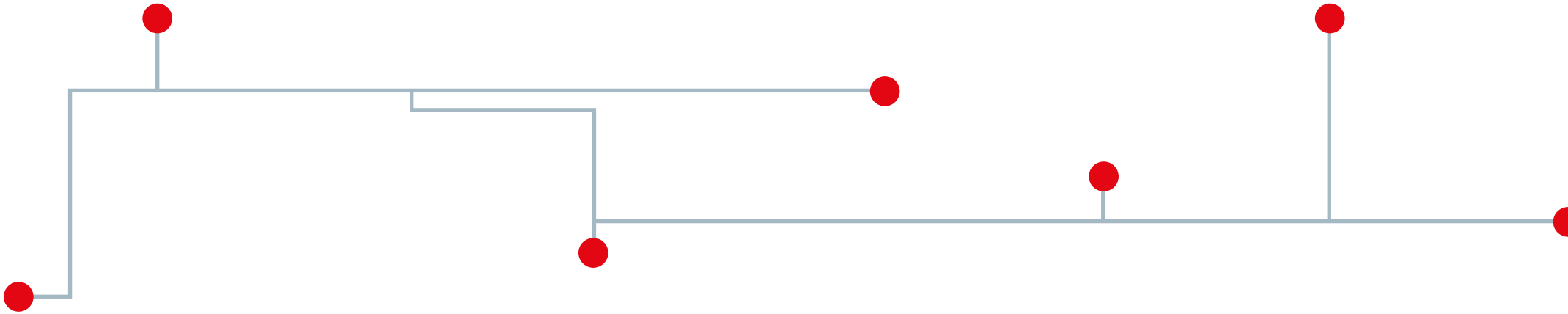
Resource

Depending on the nature of your business and extent of your risk exposure, you should consider whether you have the resources and skills internally to implement the necessary changes or whether you need to look to external support.

How Cripps can help

We will look at your data map and any documentation you have provided to understand how your business uses data and then we will:

- produce a **report** on the flow of personal data within your business detailing what remedial actions (if any) you need to take
- work with you to develop an **implementation strategy** which works for your business, outlining the steps which can be taken toward compliance, both for individual processes, and your processing activities as a whole.



4 Implementation

Key considerations

Operational changes

Our recommendations from Stage 3 are likely to include changes to your processes and how data flows in, around and out of your organisation. You should ensure that key stakeholders in your business are aware of the changes which are coming as a result of the GDPR and appreciate the impact this is likely to have. We can provide guidance and liaise with you to ensure that operational changes are properly implemented.

Policy

The GDPR introduces new provisions which place a greater emphasis on the accountability and transparency principles which were originally introduced by the DPA. As such, a comprehensive and robust data protection policy is both a valuable internal resource for guidance and best practice, and evidence of compliance.

Notices

The GDPR requires certain information to be provided to data subjects by way of privacy notices, including the details of the data controller, the purpose for data capture, and how long their details will be held for. Privacy notices will need to be prepared and provided within the required timeframes.

Contracts

The GDPR sets out a number of provisions which data controllers must have in place with their data processors. This includes ensuring that the data processing is governed by a legally binding contract between the data controller and data processor.

Privacy by design

Data controllers are required to ensure that appropriate technical and organisational measures, designed to implement data protection principles, are incorporated into any data processing activity to protect the rights of data subjects.

How Cripps can help

We can use the information gathered in the initial data mapping phases to:

- develop a practical **policy** to meet the needs of your business. This could include things like staff training and reviewing HR policies
- provide **training** on data protection for your staff
- develop internal and external **privacy notices** to ensure you comply with GDPR obligations. Internal privacy notices would be used for employees (as the GDPR also applies to employee personal data) and external privacy notices would be used for all other personal data you hold
- draft variation agreements to ensure that current **contracts** are fully compliant, as well as providing template wording for inclusion in future contracts.

5 Monitoring

Key considerations

Data compliance register

At the end of the process you should compile a data compliance register – a suite of documents which evidences the different steps you have taken to achieve compliance.

Suppliers

Having reviewed your existing contracts with suppliers, you should ensure future contracts (and systems) are GDPR compliant. You will need to factor GDPR compliance into your due diligence process and ensure that any risks are identified and mitigated.

Subject access requests

Data subjects now have the right to make subject access requests (at no cost to them as a default position) and obtain information with regards to the data you hold about them. The maximum time to make this information available has been reduced from 40 days to 'within one month' (subject to some exceptions) therefore you need to consider whether there are any logistical issues in dealing with requests more quickly (including potentially a secure online system which allows subject to access their data themselves).

Assessments

If you are looking at specific data processing projects which may carry a higher risk, it is worth considering a Data Protection Impact Assessment which is an integral part of a 'privacy by design' approach and can be used to identify and reduce the privacy risks within projects.

Notifying breaches

The GDPR introduces a duty on data controllers to report certain types of data breaches to the Information Commissioner's Office, or the data subjects themselves. You will need to consider what processes you have in place for identifying, recording and responding to data breaches.

Data Protection Officer/Data Compliance Officer

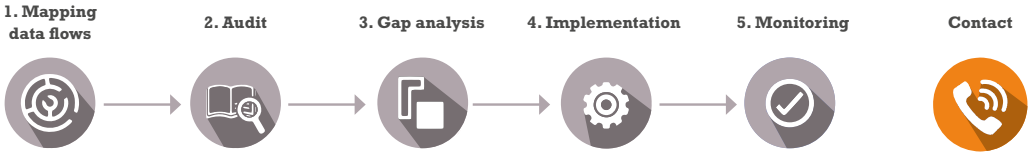
Any organisation can appoint a Data Protection Officer (DPO), however certain organisations are mandatorily required by the GDPR to do so. Their role is to provide internal guidance and ensure that your organisation is compliant with the GDPR and various other responsibilities.

How Cripps can help

Cripps can provide **on-going support** to your Data Protection Officer or others in the organisation.

We can also:

- provide a Privacy Impact Assessments template and advise on their completion
- advise on what due diligence or other practical measures may be necessary to reduce risk when entering into new agreements with third parties
- provide policies, templates, and ad hoc advice on how to deal with data subject requests around access, deletion, rectification, portability and restriction
- if you are concerned about a breach, we can provide template notifications and guidance documents and help you assess the situation and deal with it
- we can advise on, or carry out, periodic checks of your data activities to ensure you maintain compliance.



For more information

The GDPR comes into play on 25 May 2018. There is no transition or 'cooling off' period so it is imperative that you have engaged your key stakeholders, reviewed your existing policies and procedures and made the appropriate changes prior to this date.

If you would like to find out more about how we can help you, please contact:

Irfan Baluch
Partner
+44 (0)1732 224 006
irfan.baluch@cripps.co.uk

Elliot Fry
Associate
+44 (0)1732 224 034
elliot.fry@cripps.co.uk

Cripps has created a GDPR hub which provides further information and guidance on all aspects of the GDPR, **www.cripps.co.uk/gdpr-hub**.

For further information on any of the topics below please visit the hub:

- **About the legislation**
- **Internal compliance**
- **Contracts and operational issues**
- **Rights of individuals**
- **Marketing**

Cripps LLP

London
Tunbridge Wells
Kings Hill

T +44 (0)1892 515 121
F +44 (0)1892 544 878
E contact@cripps.co.uk
www.cripps.co.uk