Digital Comp☑iance Hub

GDPR Compliance Roadmap

Your GDPR Compliance Roadmap

Start here....2
Data protection & GDPR basics....3
Carrying out a GDPR audit....7
Understanding the lawful basis for processing....8
Do I need a Data Protection Officer?....9
What data protection policies do I need?....10
Data protection training....11
What do I need to put in my privacy notice?....12
What else?....12
What if the data was given to us?....12
Documenting your processing activities....13
Third-party processors....14
What if my service means I'm a third-party processor?....15
GDPR and electronic marketing....16
Data retention....18
Security of processing....19
The right to be forgotten....20
Right to data portability....21
Subject access requests....22
Data protection by design and default and DPIAs....23
HR and employee data....24
Dealing with data breaches....25
Third party access to data....26
ICO Data Controller / Processor register....27
Looking to the future....28

Start here

Thank you for downloading this Digital Compliance Hub GDPR pack. The concept for the pack is simple: to provide you with the basic tools you need to meet the requirements of the General Data Protection Regulation.

The pack is made up of this compliance roadmap document which is supported by additional documents and templates that make up the rest of the pack. You should work your way through this document as your guide to GDPR compliance and use the additional documents and templates to support your compliance.

For more detailed tools, guidance and information as well as help and support please consider joining the Digital Compliance Hub (https://digitalcompliancehub.co.uk) which provides more detailed help and support on the digital compliance challenges your business is likely to face, including GDPR.

Signing up to the Hub comes with a 14-day free trial. As part of this GDPR pack, though, you can enjoy your first month subscription for free. Simply, sign up to the Hub using your account and contact us (support@digitalcompliancehub.co.uk) to let us know and we'll apply an extra month discount to your subscription.

What if I need further help?

If you have any questions relating to the content of this pack, you can use the support functionality of the Hub to get help. If you need help with any aspect of implementing GDPR compliance within your organisation please contact support@digitalcompliancehub.co.uk to find out more about our GDPR consultancy services.

If you have any difficulties access the contents of this pack, please contact us via support@digitalcompliancehub.co.uk

What documents are included in the pack?

- This roadmap document
- GDPR Audit Registers - for recording what data, systems, processors and policies you are using
- Hub Policy Bundle – a selection of policy document templates for you to adapt for your own organisation including a data protection policy, subject access request policy, etc.
- Privacy notice template
- Data protection training presentation – for training your staff about data protection basics
- Third party due diligence checklist – for your data processors to assure you of their data protection compliance
- Data retention guidance – to help you formalise a policy for retaining your data

Data protection & GDPR basics

GDPR background

The GDPR is a new piece of European legislation which was ratified on 27th April 2016 and comes into force across the whole of the European Union, including the UK, on 25th May 2018.

Described by the UK's Information Commissioner as "*the biggest change to data protection law for a generation*" the Regulation replaces existing member state laws that implemented the previous EU data protection Directive. Despite the UK leaving the European Union the Regulation will replace the UK's Data Protection Act 1998 and will be engrained into UK law, post-Brexit, by a new Data Protection Act 2018.

Key Definitions

- "Personal data" relates to any information about an identifiable natural person (the "Data Subject") either directly or indirectly
- "Processing" means any activity carried out on the personal data including storage, collection, organisation, manipulation, destruction and general use
- A "Data Subject" is the person whose data it is that is being collected or processed by the Data Controller and/or the Data Processor
- "Data Controller" is an organisation who determines the purposes of processing of data – typically this is the organisation that has collected the data in the first place and wishes to process it
- "Data Processor" is an organisation who processes data on behalf of the Data Controller (typically a third party)

Main GDPR Changes

The GDPR introduces several new data protection concepts as well as updating existing EU data protection law to meet the challenges of a digital age. The main changes can be summarised as:

- Applies to all EU member states with only a few options for derogation
- Applies to any organisation outside the EU delivering services or products to EU citizens
- A wider definition of "data" to include online identifiers (such as IP addresses and social media handles)
- Increased accountability for Data Controllers and Data Processors. It is up to those collecting and/or processing data to be able to demonstrate they are acting within the rules. This means in some circumstances records must be kept and processes documented.
- Stricter rules for collecting consent for the purposes of processing data. Consent for processing now needs to 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*"
- Specific rules for consent related to children using online services (defined as under-16 in the Regulation, although member states can define their own age limit provided it does not drop below 13)
- Changes to Data Subjects' rights, including two new individuals' rights:
    - The right to be informed provides a prescriptive list of details that must be provided to Data Subjects at the point of data collection (or before use of third party data)
    - Changes to the Data Subject access right – information must be provided free or charge and within 30 days (charges only available in certain circumstances)

    - The right to the erasure of all data a Data Controller may hold (the right to be forgotten)
    - The right to data portability. This right allows a Data Subject to request a copy of their data in machine readable format either for their own processing or to import into an alternative service (perhaps provided by a competitor)
- New responsibilities for Data Processors in terms of liabilities
- Data Controller – Data Processor controls in place including contractual terms and the responsibility for the Data Controller to use only processors able to guarantee compliance
- The introduction of the concept of data protection by design. This requires all processors of data to consider the ramifications on the privacy and data of the Data Subjects of new products and services. Data Protection Impact Assessments ("DPIA") should be used as a tool to ascertain data protection by design within individual projects, or where there is "high risk" to the data subjects
- The requirement for some organisations to appoint a Data Protection Officer ("DPO") to take specific responsibility for data protection. Not every business will need a DPO but for those that do, the GDPR has specific rules about the role of the DPO within the business.
- The requirement, under certain circumstances, to report a breach of data protection to the national regulator (the ICO in the UK) and Data Subjects. The requirement to report a breach is most likely to be needed when there are large quantities of data breached or when the breach is likely to cause significant harm to the Data Subject.
- Increases in fines. Under UK law the current fine threshold is £500,000. Under the GDPR there are two thresholds of fine; the highest is 4% of global turnover or €20m, whichever is the highest (although it should be noted that the ICO has indicated that we're likely to see maximum fines).

Data Protection Principles

Whilst the list above sets out the main changes to data protection regulation introduced with the GDPR, the main framework for data protection remains with the GDPR as it does currently with the UK's Data Protection Act 1998. At the heart of this data protection framework are the data protection principles, which in the GDPR, state that data must be:

1. Processed lawfully, fairly and transparently
2. Collected only for specified or legitimate purposes and not further processed outside the original purpose for collection
3. Relevant and necessary for the purposes for which they have been collected (i.e. don't collect data you don't need)
4. Accurate and kept up to date
5. Only kept for as long as the data is required. Where data is no longer required it must be deleted or anonymised
6. Kept and processed securely

And, underpinning these six principles is the principle of "accountability" meaning it is up to the controller to demonstrate its compliance with the principles.

The Data Protection Act principle relating to transfer of data outside the EU is covered in Chapter V of the Regulation and relates to controls over how EU citizen data is processed outside the EU.

Lawfulness of Processing

Article 6 of the GDPR sets out the ways processing of personal data is considered lawful:

1. Where the Data Subject has given consent
2. Where processing is required for the performance of a contract
3. Where processing is required to comply with a legal obligation
4. Where processing is necessary to protect the vital interests of the Data Subject
5. Where processing is carried out in the public interest
6. Where processing is carried out in the legitimate interests of the Data Controller, but without detriment to the Data Subject

Consent

Consent is defined in Article 4(11) as "*any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*;". This defines the conditions by which consent would be considered lawful for processing. The GDPR also sets out that

1. The Data Controller should be able to demonstrate that consent was given by the Data Subject
2. Where consent forms part of a wider amount of information it should be distinguishable from the other material
3. Consent can be withdrawn at any time by the Data Subject

Processing of Special Categories of Data

Special categories of data relate to data as defined in the Data Protection Act as "sensitive personal data". Specifically, "*data relating to 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*". Data that falls into this category can only be processed if one of these conditions are met:

1. Explicit consent has been given by the Data Subject
2. Processing "*is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the Data Subject in the field of employment and social security and social protection law*"
3. Processing is in the vital interest of the Data Subject
4. The data is in the public domain
5. Processing is in the public interest
6. Processing is necessary "*for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services*"

Data Subject Rights

Under the GDPR Data Subjects have the following rights:

1. The right to be informed (including when the data was not obtained directly from the Data Subject) about who has their data, what it's used for, who will have access to and their rights to object, withdraw consent, etc.
2. The right to request whether data is being processed by the Data Controller and if so what data and how (this is a Subject Access Request)
3. The right to have their data updated and kept up to date
4. The right to erasure of their data when the data is no longer needed, when consent has been withdrawn or if it has been unlawfully processed
5. To restrict, in certain circumstances, the processing of their data
6. The right to data portability allowing a Data Subject to request copies of their data in a format compatible with another system for their own use or to import into a third-party system
7. The right to object to the processing under legitimate interests, for direct marketing purposes, for profiling or research
8. The right to object to automated decision making

The Controller – Processor relationship and third parties

The GDPR requires:

- A Data Controller to only use a Data Processor if it is sure they are GDPR compliant and thus, by implication, enabling the Controller to maintain compliance
- A contractual relationship between the Controller and Processor, with the GDPR specifying specific terms that must be in place

So, for a Controller this means:

1. They will need to carry out due diligence on any third-party suppliers who process their data
2. They will need to make sure the required contractual terms are in place in contracts between them and the Processor or within the Processor's terms

And, in situations of a Processor processing data on behalf of their clients:

1. They can expect their clients to carry out due diligence on them
2. They will need to update their terms of service to meet the contractual requirements, or expect to review updated contracts from their clients

When it comes to third party processors, you should be mindful of the definition of processing covering everything that you do with that data including storage, so this will include third party services such as data hosting and storage, outsourced marketing, software applications running online (SaaS and cloud services), outsourced payroll to an accountancy firm, etc. When dealing with cloud-based services it is also particularly relevant to consider where your data will be stored – if the service is US based or the data hosted elsewhere outside the EU then you need to be sure you meet the international transfer of data principles of GDPR relating to adequacy or lawful contractual terms.

Carrying out a GDPR audit

One of your first steps, once you've got a rough grip on what data protection means for your business is to understand more about your business in terms of the data you process, how you process it and your current data protection policies.

Audit templates are available as part of this pack. You'll understand more about how to use some of the columns and what actions you need to take as you go through this roadmap document.

- ☐ Audit your data to understand what data you have, who it relates to, what kind of data it is and where you process it
- ☐ Audit your processes and processors (real and digital) to understand where your data is being processed. Here you will need to record where your data is being processed, which may be by real people or online or digital systems
- ☐ Audit your current policies and documentation that make reference to data protection

What do I need to put in my privacy notice?

Privacy notices or policies have an important role in GDPR compliance as they're the best placed tool in most cases to meet the requirements under GDPR regarding transparency of processing and the individuals' right to be informed. You should include:

- ☐ Your identity and contact details and the contact details of your data protection officer if you have one
- ☐ The reason you are processing the data
- ☐ The legal basis for processing including details of any legitimate interests you are relying on
- ☐ Who you share the data with (if at all)
- ☐ Details of any data transferred outside the EEA and your assessment that adequate data protection practices are in place
- ☐ Detail, where possible, of your retention periods for the various pieces of data
- ☐ The individuals' rights with regards to their data
- ☐ How they can complain to you and/or the regulator (ICO)
- ☐ Any consequences of not providing data (where it is needed, e.g. for fulfilling a contract)
- ☐ Any automated decision-making practices being used on the personal data
- ☐ Details of any cookies or tracking code/pixels being used, unless covered by a separate cookie notice

What else?

- ☐ Our privacy notice is easily found on my website
- ☐ Our privacy notice is easy to understand and access
- ☐ Our privacy notice covers a wide range of processing activities (e.g. customers, people who contact us, data collected from our website, employees, etc.)
- ☐ We sign-post our privacy notice at every point we collect data
- ☐ Where we have changed an existing privacy notice and indicated we would communicate changes to those affected by the notice, we have communicated the update privacy notice to the data subjects

A templated privacy notice is available as part of this pack.

What if the data was given to us?

- ☐ We provide a privacy notice setting out how we came by the data and what we will be using it for
- ☐ In addition, we provide the same information as in our main privacy notice
- ☐ We provide the information within one month of having access to the data