

Getting data protection right: new legal changes



The laws relating to how organisations should deal with an individual's personal data is about to change dramatically. Organisations need to prepare now for these changes.

The Information Commissioner is forging ahead with General Data Protection Regulation (GDPR) implementation plans, and further guidance on how to interpret the provisions of the Regulation is expected to be published in the foreseeable future.

As a consequence, those organisations that haven't started reviewing their existing data protection measures will need to take urgent action over the coming months in order to ensure they are compliant.

DWF's data protection experts have the experience and knowledge to guide you through the various challenges that arise from the GDPR. We understand that budgets are limited and pragmatic commercial decisions will have to be taken. You will need to take pragmatic commercial decisions about what the key risks are to your business and we can provide you with the strategic advice, practical tools and assistance that you require in order to do this.

How DWF can help you prepare for GDPR – Piecing together compliance:



Audit & Gap Analysis Review

We can provide a range of services to suit your organisation's needs and budget. This might be a simple high level 'Compliance Checker' action list, a more detailed gap analysis survey which we assist in the completion of or over the phone support to enable your organisation to conduct its own survey internally. We recognise that budgets are not limitless and so we can help you identify the most important areas that you should address.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are an important component in achieving compliance. Whilst previously they were recommended as representing good practice, the need to undertake PIAs will become a legal requirement under the GDPR. They are used to evaluate the potential risks posed to an individual's privacy rights through particular uses of personal data.

We can assist with the drafting of PIA templates for use in all new data processing projects within your organisation. Often the reality is that organisations do not have the resource for legal or compliance to sign off all PIAs.

Our training solutions can help equip appropriate operational staff to conduct self-certified assessments and provide risk ratings based on your particular type of business and data processing activities, so that closer scrutiny by legal or compliance functions is triggered where appropriate. We can also steer you through specifically complex PIAs for example, where sensitive or high volumes of personal data are involved or where the risks to data subjects are particularly high.

Governance and Compliance Documentation

Organisations must be able to demonstrate that compliance is practised from the executive level, through to business heads and senior managers and down to the operations and customer facing staff who are handling personal data on a day-to-day basis.

It is important that governance frameworks take in all functions within the organisation that involve the handling of personal data. This is often achieved through a data protection steering group.

We can provide you with terms of reference and overarching framework documents to help you demonstrate governance within your organisation.

We can also provide template key compliance policies to reflect GDPR standards, such as those detailed below, or conduct gap analysis reviews on your existing policies:

- General data protection policy
- Human resources data protection policy
- Subject access policy
- Data security breach response policy
- Acceptable use policy
- Social media policy
- Bring your own device policy
- Information classification policy
- Data retention policy
- CCTV policy
- Direct marketing guidelines
- Third party disclosure request guidelines
- Remote access policy
- Confidentiality policy
- Data sharing checklist

Training

The employees who work within an organisation need to be sufficiently aware of their data protection obligations. With fines of up to the greater of 4% of global annual turnover or €20 million, you should ensure that the people in your business are fully trained on all aspects of the GDPR.

All organisations will have changes to make to their policies, processes and procedures to bring them in line with the stricter new requirements. We have created some training courses which are designed so that you and your employees are aware of the principles of the Regulation, and understand what actions are required to manage the risks at their level. Our training courses are available in half day and full day sessions.

Data Mapping and Cataloguing

Understanding the types of personal data that are collected by your organisation, the records and systems in which it is stored, and why and how it is used, is important to ensuring compliance.

Whilst operational staff may generally have a good understanding of how personal data is processed and stored within their own department or function, there is often no single organisational wide view of this.

Given the significance of new pseudonymisation provisions in the GDPR, and the increasing trend for leveraging commercial benefit from analytics drawn from personally identifiable records, a holistic approach is essential.

We can help train your staff to understand the legal and commercial significance in understanding the difference between pseudonymised and anonymised data, and to help position the differences.

We can also assist with survey questionnaires to help obtain that important single view of the organisation's personal data assets.

Our expertise

- Strategic compliance advice ranging from informal 'on the ground' assessments through to compliance audits, gap analysis reviews and governance frameworks.
- Data security breach prevention and response.
- Building privacy compliance into new projects.
- Handling ICO complaints, investigations and formal enforcement actions; assisting in the defence of privacy claims made by individuals and group actions.
- Maximising the value of customer data for direct marketing, customer profiling and big data initiatives.
- Managing personal data and protecting risks throughout the supply chain.
- Specific industry expertise such as retail, insurance and consumer finance sectors.
- Global data transfers and managing intra group data sharing.

Get in Touch

If you would like to discuss any of the above issues, or learn more about our services, we would be delighted to hear from you.



John Benjamin
Partner
T +44 (0)20 7280 8950
E john.benjamin@dwf.law