DATA PROTECTION - 10 STEPS TO COMPLIANCE

Are you responsible for data protection within your organisation? If so, you will know just how much data protection information there is on the internet. At times, it can be overwhelming and time consuming to digest. Your data protection compliance can sometimes slip down the 'to do' list.

The trick to ensure effective compliance with business regulations and data protection is to adopt a logical 'keep it simple' approach. Look at it as an opportunity to benefi t and add value to your organisation, rather than being a box ticking exercise.

So, here are my top tips on what is essential for data protection compliance:

1. Data audit

Ask yourself -

- whose/what personal or sensitive personal data do you hold (this includes staff and customers);
- how/where is it stored?
- who has access to it?
- for how long is it stored and for what purpose?
- who are the data controllers and/or processors?

Record your answers for future reference.

2. Risk assessment

What are the risks associated with the data storage and what are you going to do to eliminate those risks or reduce them to the lowest level possible? Risks might include a lack of understanding of what is meant by personal (or sensitive personal) data, loss of personal data, home working, disclosing personal data in error, failing to identify a request for access to personal data, retaining data for longer than is permitted or for a non-specific or irrelevant purpose, a change in personnel, new projects, a failure to register with the Information Commissioners Office or personal data being held by third parties (for instance, in the cloud). Again, you need to record your findings and feed them into your risk register and training sessions.

3. Privacy policy

Set out what the organisation intends to do about protecting individuals' personal data and the key personnel with responsibility for data protection - this does not need to be War and Peace!

4. Procedures

What practical steps are you as the data controller going to take? You will need to have in place procedures to deal with issues identified in the risk assessment such as:

- Data security
- Data access requests - covering in particular, to whom any (or any suspected) requests should be directed, ensuring the identity of the person making the request is clear, how to deal with third party information held with the personal data requested (this can be particularly tricky), reasons for denying access to personal data and how you record relevant deadlines and decisions (for instance to deny or permit access to personal data)
- Taking of/use of photographs or CCTV

- Disposal of data
- What to do in the event of a breach or suspected breach of the Data Protection Act - covering who will conduct the investigation, who should be contacted (this might include the individuals concerned, Information Commissioner's Office, your lawyers and insurers), whether internal disciplinary action is required and dealing with any adverse media coverage (you will no doubt find there are cross references to other documents, such as your social media policy, staff handbook/employment contracts and so on)

It might seem like a long list but with a little thought, procedures can be kept concise and manageable. It is often a good idea to involve staff who either already have or are likely to have hands on experience of data protection issues as this often leads to the development of more relevant and robust procedures as well as better buy-in from staff.

5. Training

Ensure anyone who handles or is likely to handle personal data is fully conversant with what the organisation and their colleagues expect from them.

6.Standard templates and documents

Draft and use these for subject access requests (if you want to put it on your website) and responses to subject access requests.

7. Communication

Ensure prompt and transparent communication with staff and customers about data protection issues, including 'plain English' privacy notices.

8. Contractual Arrangements

Have in place proper contractual arrangements with third parties holding or disposing of personal data - to ensure clarity of the identity of the data controller/processor and who has responsibility for what as well as inclusion of appropriate confidentiality and liability/indemnity clauses.

9. Keep everything under review

As a benchmark, an annual review is sensible, although if there are any significant changes during the year, you should revisit your policy and procedures to ensure they remain relevant. Monitoring can help with improving and streamlining processes.

10. Keep up to date

Think about signing up to a regular update to save time. This is especially important with the EU Data Protection Regulation on the horizon.

Once established, data protection policies and procedures will become an integral part of the day to day running of the organisation rather a burden. As well as the benefits already alluded to, you will have staff that are confident of what they can and can't do, it will help build trust with customers and the reputation and financial position of the organisation will be protected.

Find out more

Please contact us to discuss your requirements or to find out more.

Laura Trapnell

Head of IP
023 8048 2114
laura.trapnell@parissmith.co.uk

Cliff Morris

Partner
023 8048 2289
cliff.morris@parissmith.co.uk