Data Protection Legislation

GDPR - What, why, who and when?

What is GDPR?

GDPR is the EU General Data Protection Regulations 2016, which come into force on 25th May 2018 and replaces the Data Protection Act 1998. This is unaffected by Brexit – it is already UK law, and needs early attention.

What has changed?

Though the new legislation builds on existing principles, there is a considerable level of change in practice, including the following:

- additional rights for individuals including the right to have their data changed or deleted, and the right to take their data somewhere else
- increased obligations to record what steps you are taking, what assessments you've made
- a new Accountability Principle, and an obligation of transparency, both of which require active steps
- changes required to the processes for taking consent, and the information you have to give
- appoint a designated Data Protection Officer, who will probably need to be at Board level, and report to the Board – and be obliged to report breaches to the Information Commissioner's Office (ICO).
- The fines are going up from a maximum of £500,000 to either 4% of global turnover and €20 million (whichever is greater)

What do I have to do?

You have to take the necessary steps – both organisational and technical. The ICO says there are these twelve steps (these are the ICO's words*):

1. You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have
2. You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit
3. You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
4. You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information
6. You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it
7. You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity
9. You should make sure you have the right procedures in place to detect, report and investigate a personal data breach

GDPR comes into force on 25th May 2018 and needs early attention.

10 You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation

11. You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12. If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

*Information Commissioner's Office, "Preparing for the General Data Protection Regulations (GDPR): 12 Steps to take now v2.0 20170525", licensed under the Open Government Licence

Why is this coming into force?

The world, and the mechanisms for collecting data have changed enormously since 1998. The opportunities to abuse the personal data of individuals has increased beyond any expectation, so the objective of GDPR is to protect the rights of individuals, by encouraging, and requiring businesses to comply.

Who can help?

This will depend on each business, and you may be able to do the necessary work yourself; or you may need legal advice to understand and prepare the governance requirements, legal notices, consent etc; consultancy assistance in putting systems in place; and technical input from your technology providers. As specialist technology lawyers dealing with the protection of data and rights for our clients, we have been dealing with data protection for many years.

Why do I have to do anything?

- This affects all businesses, regardless of size, but in different ways (you need to understand in what ways it affects your business)
- It doesn't just affect businesses dealing with consumers – it affects business to business companies too
- You need to make sure you are fully in line with the new regulations
- You need to ensure that the Board of the company is aware of the new regulations, the need to deal with them at Board level, allocating the resources for proper education, training, advice and for making necessary changes
- ICO will have enhanced powers of enforcement
- If you don't protect the data of individuals, your business can suffer substantial financial and reputational damage.

When do I have to do it by?

25th May 2018 – but give yourself time to work through what you need to do, because doing it as a last minute rush will take a lot of time and resource; which you may not have

August 2017 – This note does not constitute legal advice.

To discuss Data Protection with us, please contact
Head of Commercial and Digital, Paul Berwin

☎ 01423 542 777
paulberwin@berwin.co.uk
berwin.co.uk/digital
@paulberwin

GDPR – actions for you and your organisation(s)

Organisations need to take the necessary actions relating to GDPR, with the benefit of external advice where necessary. Each organisation's requirements will be different, but for all the function should be conducted independently of commercial and decision making channels.

Steps to ensure General Data Protection compliance	Internal	External
Ensure that the Board of the company: •is formally made aware that GDPR makes Data Protection a board-level responsibility, and not limited to an IT or HR issue;	X	
•is itself aware and trained in GDPR requirements;		X
•is aware of the need to allocate the necessary resources in terms of cost, skills, training and time to the GDPR process on an ongoing basis	X	
Undertake a comprehensive data mapping analysis to identify and record key aspects of the process		X
Create an action plan, with external advice where beneficial, to achieve GDPR readiness. This should include the resources, costs and training	X	X
Procure Board approval: •for the action plan and resources;	X	
•the appointment of a Data Protection Officer (or equivalent)	X	
Proceed with the documentary requirements, with legal input, including: •internal policies	X	X
•consent checklists and notices wherever required;		X
•privacy notices;		X
•contractual provisions with suppliers;		X
•dynamic register to cover all data processing activities;		X
•breach notification procedure;	X	
•subject access request procedure;	X	X
•Data Protection Impact Assessment procedure;	X	X
•Privacy by Design procedure.	X	
Put in place processes for ongoing reporting and training to the Board	X	
Organise and arrange delivery of whole-organisation training		X
Implement an ongoing compliance overview and review process	X	

Contact Berwins' specialist team to discuss your GDPR compliance
01423 542 777 • paulberwin@berwin.co.uk