General Data Protection Regulations

BRIEFING PAPER

East Midlands Chamber
Derbyshire
Nottinghamshire
Leicestershire

Introduction

The General Data Protection Regulation 2016 (GDPR) become law in all EU member states, which includes the UK, on 25 May 2018.

Because all EU regulations in force at Brexit will be assimilated into UK law, GDPR will be enforceable in Britain for the foreseeable future and is being looked at as a future global model for data protection.

GDPR will be assimilated into UK law, with tighter controls and significantly greater penalties

GDPR is intended to secure more transparency for data subjects and aims to improve consumer trust.

But it brings with it considerably tighter controls over the processing of data, how data can be used, the rights of individuals on whom data is processed and significantly greater penalties for not protecting that data.

It is, therefore, imperative that you understand the implications of GDPR and ensure you adopt appropriate protocols to ensure compliance.

Why are data protection rules changing?

The existing data protection legislation was drawn-up in the 1990s, at a time when smartphones, search engines and social media didn't exist.

First real change to data protection laws since the 1990s

Organisations are now in possession of more customer information than ever before. As the 'data stack' grows, regulators recognise that existing laws – which are different for each of the 28 EU member states - were insufficient to manage how the data and its use were governed.

Put simply, the changes introduced by GDPR are intended to:

- harmonise data protection laws across the EU
- reflect increased use of technology and the internet, and
- provide data subjects with improved rights and greater transparency about the way information is managed.

Data subjects will have improved rights

Why should I worry now?

GDPR comes into force at the end of May next year. So do the penalties for non-compliance.

Evaluating the potential impact of GDPR on your business, implementing the necessary changes to your processes and, if necessary, IT systems and training your staff, will take time.

Evaluating the potential impact of GDPR needs to start now

It is recommended that you begin preparations for GDPR as soon as possible.

What happens if I don't comply?

It is imperative that you view your obligations under GDPR in the context of the size of the fines for non-compliance.

Non-compliance could result in huge penalties

In the UK, the maximum fine for a data breach under the current Data Protection Act is £500,000. Under GDPR, the maximum fine for non-compliance could be:

- 20m euros or
- 4% of annual global turnover.

20m euros or 4% of global turnover

You might also miss out on the opportunity to more accurately target new customers and suffer reduced efficiency.

What do I need to know?

1. Current data protection regulations apply only to businesses carrying out data processing in the EU or where equipment is located in the EU. GDPR will apply to:

- businesses in the EU – whether or not the actual data processing takes place in the EU, and
- businesses outside the EU where:
  (i) goods and services are offered to EU subjects, or
  (ii) the behaviour of EU subjects online is being monitored.

Non-EU entities caught by the GDPR will generally be required to appoint a representative in the EU.

Non-EU companies might need to appoint an EU-based representative

Act now

- Consider if you need to appoint an EU representative – Britain won't be in the EU, remember.
- Check whether GDPR will apply to third parties you deal with
- Be prepared to review/renegotiate contracts to reflect changes.

2. Under GDPR, data processors (businesses which process data on behalf of a controller) will also be subject to statutory obligations and liabilities.

Businesses processing data on behalf of another will have statutory obligations

Act now

- Consider whether your business might have obligations under the GDPR as a data processor and, if so
- Take advice on the actions that will be necessary to comply with the GDPR and to minimise the risk of breach.

3. More of the data that you process may be 'personal' and, therefore, subject to data protection laws because GDPR clarifies what 'personal data' will usually include.

Under GDPR, sensitive personal data (referred to as 'special categories') will include genetic and biometric data.

Personal data might include genetics and biometrics

Stricter rules will apply to the processing of sensitive personal data.

Act now

- Look at whether more of your data processing will be caught by GDPR and make sure it is included in compliance plans
- If necessary, introduce new procedures to ensure that genetic and biometric data are treated as 'special category'.

4. Under GDPR, far more information will need to be available to data subjects, including:

(i) details of the legal basis on which you process data,
(ii) where processing is justified on the basis of your legitimate interests, what those legitimate interests are, and
(iii) the intended data retention period.

The information must be provided in a concise, plain language.

Act now

- Strengthen privacy notices to reflect new requirements
- Consider changes to privacy notices to meet transparency requirements
- Make sure you comply with the timescales for provision of information.

Stronger privacy notices might be needed

5. You will not need to notify the Information Commissioner's Office about your data processing or pay fees, but you will have to keep detailed records to evidence compliance if asked. Records will need to include:

(i) the purposes for which data is being processed
(ii) the data subjects, recipients and categories of personal data processed, and
(iii) where possible, time limits for erasure.

You won't need to notify the ICO about your data processing

Act now

- Make sure you have a system for keeping necessary internal records and keep evidence of steps you take to comply with the GDPR, including any risk assessments.

You may need new internal procedures

6. Under existing regulations, one of the ways in which businesses can justify their processing of personal data is by obtaining the consent of the data subject.

GDPR introduces requirements that processing consent must be given by a clear, affirmative act, establishing unambiguous indication of the data subject's agreement. Silence, pre-ticked boxes and inactivity will not constitute consent.

No pre-ticked boxes - consent will require affirmative action

GDPR also specifies that it must be as easy for data subjects to withdraw consent as it was for them to give it and to have data erased and 'forgotten'.

Act now

- Familiarise yourself with the consent requirements and update your processes
- Review existing consents and obtain new where necessary
- Make sure data subjects can easily withdraw consent
- Consider whether there are grounds for processing that you can rely on instead of consent.

You will need to comply with transparency requirements

7. Data subjects will have more rights under GDPR to stop data processing from taking place.

They will have specific rights to have data erased (without the need for a court order).

There will be rights in certain circumstances to have personal data transmitted by one controller to another (known as the right of "data portability").

More information must be supplied to data subjects if a subject access request is made and the time limits for compliance have been reduced.

Data subjects will have right to have the use of personal data restricted while a complaint is being dealt with.

You may need to provide more information to justify the data you process

Act now

- Train staff in relation to the new rights
- Ensure your IT systems can cope with the new rights

8. Under GDPR there will be a mandatory requirement to report data breaches to the ICO and data subjects in certain circumstances and there will be tight controls on how quickly it takes place.

Mandatory requirement to report data breaches

Act now

- Familiarise yourself with the new requirements
- Implement suitable internal procedures

9. Under GDPR, for companies processing "large" amounts of data, it will be mandatory to appoint a data protection officer (DPO).

May need a data protection officer

Demand for people qualified to be a DPO will be high – 31% of firms are expected to try to recruit a DPO between now and May next year.

Act now

- Acquaint yourself with the circumstances in which a DPO must be appointed and factor recruitment into business plans and budgets.

10. Under GDPR, there will be far greater emphasis on accountability and to demonstrate compliance.

Greater accountability

As a result, certain practices that have been encouraged by the ICO for some time will become a legal requirement under GDPR, such as, privacy impact assessments and data privacy by design and default.

Data privacy by design means making sure that new data processing systems are designed from the outset to comply with all aspects of the GDPR.

Data protection by design and by default

Data privacy by default means that only data which is necessary for each specific purpose must be processed.

Data protection impact assessments will have to be carried out by data controllers before starting any processing likely to result in a 'high risk' to the rights and freedoms of data subjects.

Data protection impact assessments in 'high risk' cases

If processing is identified as being high risk, there are obligations to liaise with the relevant supervisory authority (such as the ICO) before any such processing takes place.

Act now

- Ensure new processing systems are designed to comply with GDPR.
- Ensure that, by default, your processing systems are set to the highest security settings.

Where can I find out more?

The ICO has an overview of GDPR and will publish further guidance over the coming months - https://ico.org.uk

https://ico.org.uk

For an overview of what the implications of GDPR might be for your business visit Defining the Data-Powered Future.

Defining the Data-Powered Future

For further information on GDPR and the implications for your business, or for information on different sources of support, contact Andy.Watterson@emc-dnl.co.uk.