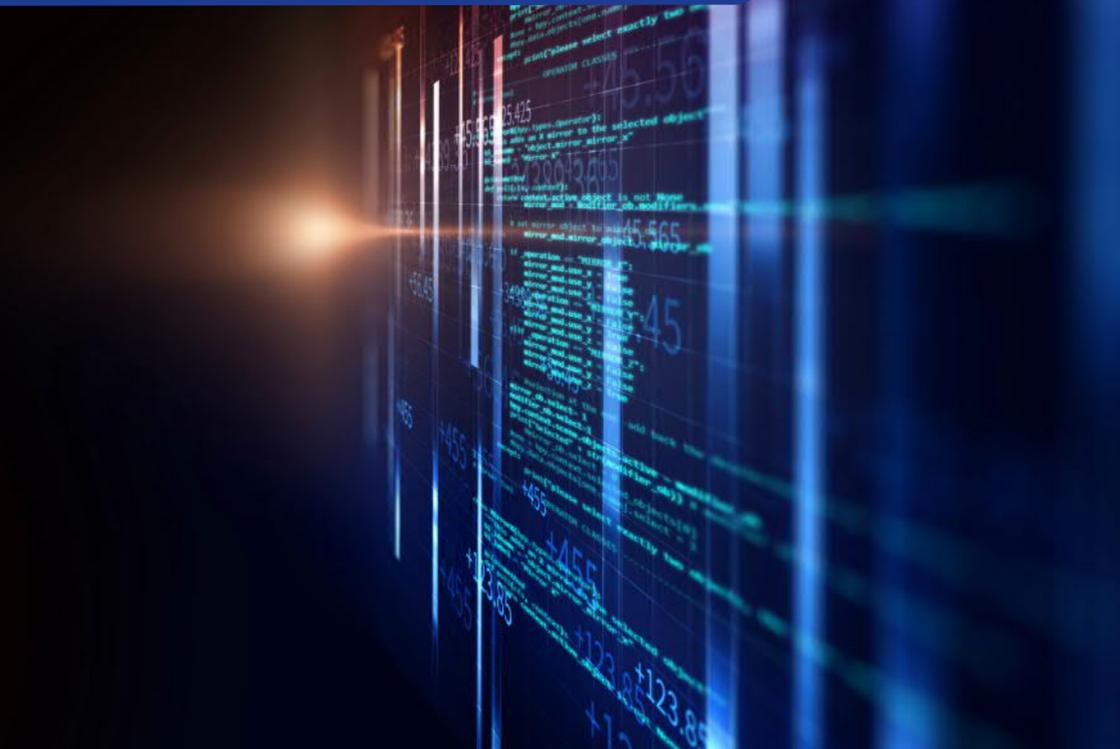


GDPR: The General Data Protection Regulation

The biggest change in data
protection law in 20 years



Introduction

The Data Protection Act 1998 (“DPA”) sets out current data protection law within the UK.

The world is now a very different place compared to when the DPA was implemented nearly 20 years ago. When the DPA came into force, the internet was still in its formative years, online banking and shopping services were taking their first tentative steps and the global social media platforms we now rely on were barely dreamed of.

As the years have gone by and technology has moved forward, ever greater numbers of people are active online in both personal and professional capacities. Increasing amounts of data and personal information are shared and, at the same time, the risk of data breaches has grown. The need for an updated, modern piece of legislation governing data protection has become increasingly obvious.

The General Data Protection Regulation (“GDPR”) is coming, the biggest change in data protection law in 20 years

Contents

- 01 Introduction
- 03 Get ready for big changes to data protection laws in 2018
- 04 International element
- 05 Individuals’ rights
- 06 Data processors & controllers
- 07 Consent
- 08 Procedures
- 09 Enforcement
- 10 Data breaches
- 10 Implementation
- 11 10 point action plan
- 12 Contact our expert legal team

Get ready for big changes to data protection law in 2018

The European Union recognised the need for an update in data protection law and the General Data Protection Regulation 2016 (“GDPR”) will be coming into force across the European Union on 25 May 2018.

As the United Kingdom will still be a part of the EU at that time, the GDPR will soon form part of our domestic law and a new Data Protection Bill was announced in the Queen’s Speech on 21 June 2017.

But what does this all mean for businesses, employers and public bodies? Brachers’ team of data protection specialists can provide expert advice to help you prepare and take a proactive approach to these far-reaching changes.



Action

Lookout for our handy action points highlighted throughout the booklet



Even once the UK has left the European Union, it seems likely that the provisions of the GDPR will remain part of domestic law.

Enforceable from May 2018 and is highly likely to apply to many UK businesses



The international element

The GDPR will have a wide territorial scope, meaning that organisations far beyond the EU could have to comply with it.

It will apply to organisations that are based within the EU but also to those based outside the EU if:

- they offer goods or services to individuals who are based in the EU; or
- if they monitor activities carried out by individuals inside the EU (e.g. spending habits).

The GDPR also allows data transfers to take place to non-EU countries only in certain circumstances including if the European Commission has made an “adequacy decision” in respect of the levels of safeguarding of data within that country.

Only a handful of countries currently benefit from this recognition and the UK will want to ensure that on leaving the EU it too is deemed “adequate” and continues to be able to receive data from the EU without problems.

Given all of the above, even once the UK has left the European Union, it is likely that GDPR’s provisions will remain part of our domestic law.

This will meet the dual purpose of safeguarding individuals’ rights and allowing UK organisations to continue to operate freely with the EU from a data protection perspective.

Many UK businesses will therefore need to be compliant with the GDPR (as well as our domestic legislation) even after Brexit – and could face stiff penalties if they are not.

Individuals' rights

The GDPR strengthens the rights and protections of individuals. Given the much wider scale upon which data is processed today, the increased risk of cybercrime and the increased awareness individuals have of potential privacy issues, this increased protection is a key focus of the GDPR.

Among the rights which can be found in the GDPR are:

The right to be forgotten

Allows individuals to ask data controllers to erase their personal data in certain circumstances.

The right to be informed

This is one of the biggest new areas requiring extensive information to be given to individuals ("data subjects"). This will include, amongst other things:

- the reason data is being processed;
- any recipients of the data;
- how long the data will be retained for; and
- the rights the individual has.

Where data is not received directly from the data subject, the data subject needs to be told about what information is held, where it has come from and how the organisation intends to use it.

The right to restrict processing or object to processing

The GDPR gives individuals enhanced rights to restrict the processing of their personal data.

The right to data portability

Allows personal data to be transferred in a "commonly used and machine readable form" to allow individuals to use their personal data across various services, e.g. to give to a different company or service provider.

The right to receive information about automated decisions

The GDPR gives individuals enhanced rights to receive explanations of how their data is used to make automated decisions about them, e.g. whether or not to approve them for a service, whether to contact them about a certain offer, etc.

! Action

Review and update your policies and procedures to ensure that they reflect the individuals' rights that the GDPR confers.

! Action

Ensure that the format in which you store personal data is workable and allows you to access and extract data both quickly and thoroughly in the event that you are called to do so.



Data controllers & processors

Beyond the rights individuals have under the GDPR, greater obligations are placed on data controllers and data processors in terms of their transparency and accountability.

In many ways, it is this aspect of the GDPR that will require the most thought, consideration and work on the part of those dealing with personal data.

The Data Protection Officer

Public bodies and organisations monitoring individuals or processing sensitive data on a large scale will have to appoint a Data Protection Officer (“DPO”).

What is meant by “large scale” is yet to be fully explained, but factors are likely to include the number of data subjects, the range and volume of data, the permanence of processing and the geographical scope.

That individual will need to be

suitably qualified and will need to be an expert in data protection law, although there are no specific qualifications they are required to have.

The DPO will be responsible for data protection and privacy within the organisation.

The DPO will need to act independently and not have duties which conflict with the role (for example, senior management, HR or marketing positions) and will need to report to the highest level of management within the organisation.

Even where an organisation is not required to appoint a DPO, having someone who has overall responsibility for data protection is advisable and should help to improve overall compliance.

! Action

Assess and if necessary appoint a DPO or other individual whose responsibility it will be to oversee data protection within your organisation.

! Action

Ensure that your DPO has received all necessary training to allow them to undertake the role and that a sufficient budget is set aside to access any additional support they will need both prior to the GDPR taking effect and in the future.

Consent

Much of the personal data that is currently processed both in a commercial and employment context is currently processed legitimately on the grounds that the subject has consented to its processing. Such consent may not necessarily have expressly been given.

The GDPR will continue to recognise consent as a legitimate basis for processing data but imposes a much more onerous obligation to obtain express consent. Such consent must be a “clear affirmative action” and be “freely given, specific, informed and unambiguous.”

“freely given,
specific, informed
and unambiguous

Consent should no longer be assumed (for example, via pre-ticked boxes on websites) nor should it be contained within wider written agreements such as contracts of employment or terms and conditions.

! Action

Identify the basis upon which all personal data is processed within your organisation. Where it is by consent consider whether there is an alternative basis for processing that data.

Any request for consent should also include details of how to withdraw that consent, and the process for withdrawing it should be just as easy as giving it.

Where data is being processed for different purposes and consent is relied upon as the reason for processing, the subject’s consent is required for each separate purpose and an audit trail needs to be kept of who consented, how and when they consented and what exactly the scope of their consent was.

It is prudent for data controllers to start considering the legitimate grounds they have to process personal data. Valid examples of processing reasons include the need to comply with contractual obligations towards the data subject, the need to comply with a legal obligation or the need to preserve or develop legitimate interests weighed against those of the individual.

“The process of withdrawal of consent should be just as easy as the process for giving that consent

Most, if not all, organisations will have work to do in ensuring they are procedurally ready for the GDPR

Action

Review and amend existing policies, procedures, contracts and other documentation which relate to data processing to ensure that all requirements of the GDPR are met.

Action

Undertake a full audit of the data collected and processed by the organisation.

Action

Review and shape your procedures in line with the data you hold and the processing activities undertaken.

Procedures

The rules within the GDPR relating to the policies and procedures organisations must have in place are complex and detailed.

Whilst the principles they are designed to promote and protect are similar to those within the current DPA, most if not all organisations will have work to do in ensuring that procedurally they are ready for the impact of the GDPR.

The onus will increase on organisations to have effective policies and procedures focussing particularly on high risk operations and processing that involves new technologies.

This may result in the need to undertake privacy impact assessments to identify high risk processing and to consult with the UK's Information Commissioner's Office ("ICO") if high risks are identified.

New obligations as part of the GDPR's procedural changes include:

- ensuring the "pseudonymisation" of data disclosed between parties
- minimising the data that is held, i.e. only holding or retaining data that is actually necessary
- implementing technical and organisational measures to facilitate compliance.

Audits of both data collected and of organisation's processing activities will be key steps to ensuring compliance.

Enforcement

The level of fines which can be imposed under the GDPR has been the headline item in press reports, and understandably so. The DPA currently caps the level of fine the ICO can issue at £500,000 which, in past cases involving global companies with enormous turnovers, was a very limited deterrent.

The GDPR seeks to ensure that data protection becomes a priority for organisations of all sizes.

The GDPR introduces a new and much higher 2-tier approach to fines which apply for particular types of infringement:

For less serious infringements

€10m or 2%

a maximum of €10m or 2% of group worldwide turnover (whichever is the greater)

Most serious types of infringements

€20m or 4%

a maximum of €20m or 4% of group worldwide turnover (whichever is the greater)

When considering historic cases involving data protection breaches, the value of 4% of group worldwide turnover for certain multinationals who have previously been involved in large scale data protection breaches is truly eye-watering.

The GDPR sets out the factors that regulators should take into account when setting the level of a fine, including:

- Was the infringement intended?
- Was negligence evident in the infringement?
- Have there been any previous infringements by the organisation?
- Did the organisation co-operate with the ICO?
- What type of personal data was affected?

The best way of avoiding fines of any level will, of course, be to ensure that your organisation complies with the GDPR.

Action

Review your commercial agreements to check for any caps on your liability and/or the liability of any of your own service providers and seek to vary any contracts that provide inadequate protection.

! Action

Ensure that staff are fully trained on how to identify a data protection breach and put in place a procedure for breach notification that ensures that breaches are reported swiftly.

! Action

Look out for updates from Brachers regarding the implementation and wording of the new Data Protection Bill

Failures to notify the ICO can result in fines at the lower level of up to €10m or 2% of group worldwide turnover (whichever is the greater).

Data breaches

In a substantive move away from the DPA rules, the GDPR will make it mandatory for data controllers to notify the relevant national authority (i.e. the ICO in the UK) within 72 hours of becoming aware of any data protection breach likely to result in material harm/or risk.

Such a notification may lead to instructions from the ICO to notify the relevant data subjects of the breach as well, a task which may be very challenging, not to mention reputationally damaging. Internal records of all data protection breaches must be kept and maintained.

Failures to notify the ICO can result in fines at the lower level of up to €10m or 2% of group worldwide turnover (whichever is the greater).

Implementation

The Data Protection Bill and the exact form it may take, may differ not only to the draft (when issued) but may also differ in some respects to the GDPR itself. Brachers' team of data protection experts will continue to monitor this situation and highlight any points where differences are likely to have a material effect.

10 point action plan

1

Make sure that the GDPR is being discussed at the top level of your organisation and that those managing the business are aware of the need to ensure compliance together with the risks of not complying.

2

Appoint a DPO or other individual whose responsibility it will be to oversee data protection within your organisation.

3

Ensure that your DPO has received all necessary training to allow them to undertake the role. Ensure that sufficient budget is set aside to allow them to do this and to access any additional support they will need both prior to the GDPR taking effect and in the future.

4

Undertake a full audit of the data collected and processed by your organisation.

5

Identify the basis upon which the data is processed and consider whether there are alternative grounds for processing the data other than relying on consent.

6

Review and shape your procedures in line with the data you hold and the processing activities undertaken.

7

Put in place a procedure for breach notification that ensures that details of any breaches of the GDPR reach the DPO or other appointed individual swiftly.

8

Provide training to all staff so that they can recognise a breach of the GDPR and are aware of who to notify.

9

Review your commercial agreements to check for any caps in your liability and/or the liability of any of your own service providers and seek to vary any contracts that provide inadequate protection.

10

Seek external expert advice where you need it. Brachers' team of experts can be with you all the way on your journey to ensure that your organisation will be GDPR compliant by 25 May 2018.

Contact our specialist legal team

Whilst the GDPR presents some new and complex challenges for organisations, it is important not to be daunted by them. With a good understanding and the right support, compliance can be achieved.

At Brachers we have a team of experts on hand who can assist you with all aspects of GDPR compliance, whether the personal data that you handle relates exclusively to your employees or extends further into your commercial practices.



Catherine Daw
Head of Employment

01622 655291
catherinedaw@brachers.co.uk



Erol Huseyin
Partner, Commercial

01622 776519
erolhuseyin@brachers.co.uk



Colin Smith
Partner, Employment

01622 776451
colinsmith@brachers.co.uk



Antonio Fletcher
Senior Associate, Employment

01622 776516
antoniofletcher@brachers.co.uk



Julie Alchin
Associate, Commercial

01622 776428
juliealchin@brachers.co.uk



Sarah Hewitt
Solicitor, Commercial

01622 776459
sarahhewitt@brachers.co.uk

Our services

Corporate

Commercial

Litigation

Dispute Resolution

Debt Recovery and Insolvency

Construction, Planning and Environment

Licensing and Health & Safety

Employment

Kent HR

Head office

Somerfield House
59 London Road
Maidstone, Kent
ME16 8JH

Call us on 01622 690691

Visit us at brachers.co.uk



@brachersllp



Brachers LLP

Maidstone | London | Discovery Park