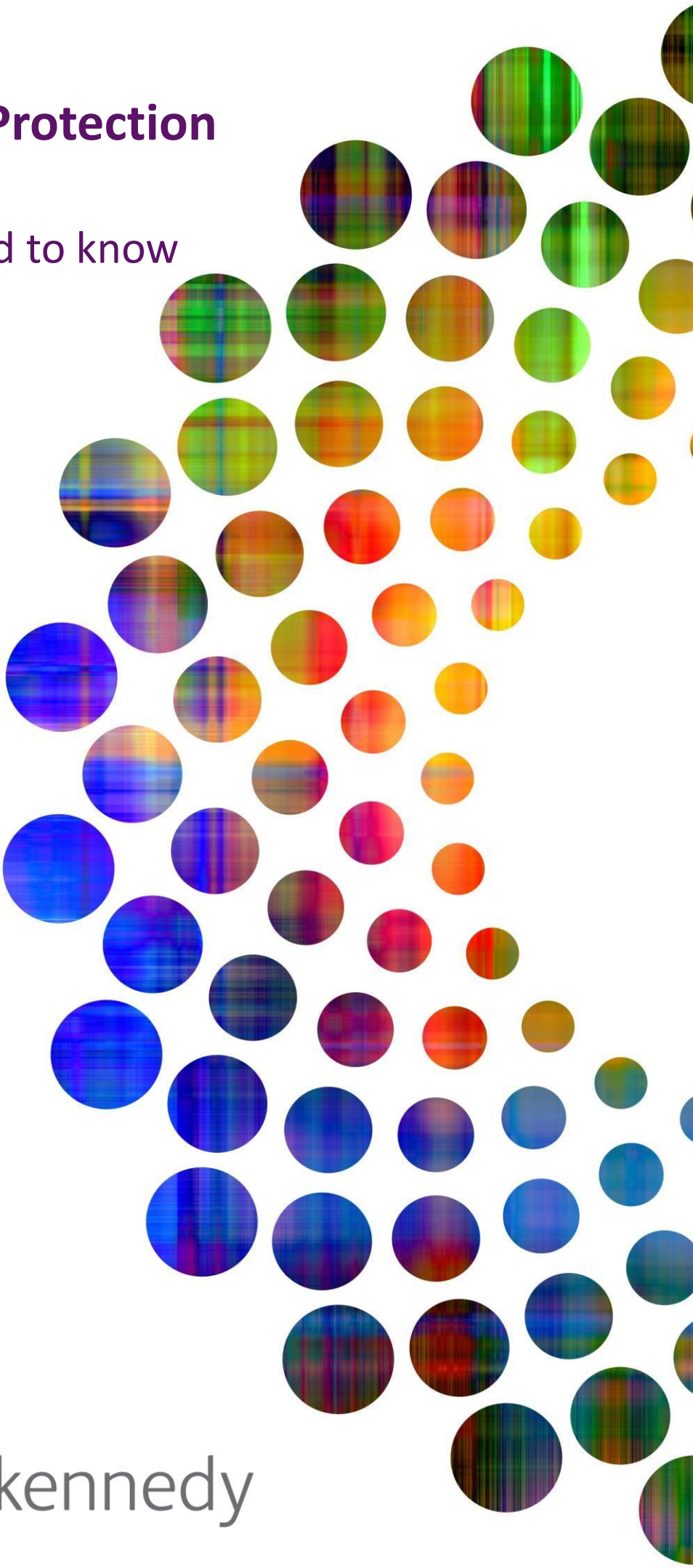
The General Data Protection Regulation (GDPR)

Top 10 things you need to know



howard kennedy

GDPR: Top 10 things you need to know

The EU General Data Protection Regulation (GDPR) is the biggest change to data protection law in 20 years. Practically every aspect of the old law has been overhauled and modernised. Businesses will need to adapt before the GDPR comes into force on 25 May 2018. As the UK will still be a Member State on this date, the GDPR will apply directly without the need for further implementation.

The Government have confirmed that the GDPR will be incorporated into the UK's domestic law on leaving the EU and must be complied with irrespective of Brexit. A Data Protection Bill is currently being passed through parliament which looks to enhance certain aspects of the GDPR and ensure the UK's continuing compliance.

We've identified 10 of the biggest changes the GDPR makes to the current law.

1. Scope

Where a business is based outside of the EU, but offers goods and services to individuals in the EU, or monitors their behaviour, the GDPR will apply. This will catch many more businesses than previously, including those based in the US and in post-Brexit UK. Also, unlike the current law, the GDPR puts obligations on data processors (organisations which work with personal data on behalf of other organisations) as well as data controllers.

Next steps: If you are established outside the EU (including in the UK following Brexit) or you act as a data processor you will have a host of new obligations. Your contracts will need to be revised.

2. Accountability and transparency

The requirement to register (notify) with the Information Commissioner's Office (ICO) will be scrapped. Instead you will have to keep full records of any data processed, including the type of data and the purpose it is used for. You will also need to give much more detailed notices to people you collect information from.

Next steps: Privacy audits and 'Privacy Impact Assessments' will be a way of life. Consider whether you should start now. Also, look at the notices and disclosures you are currently giving to your customers, these may need to be revised.

3. Data protection officers (DPO)

You may need to designate a DPO to take responsibility for data protection compliance. Their tasks will include liaising and cooperating with supervisory authorities and monitoring compliance. The DPO will need sufficient expert knowledge of data protection law and practices to conduct Privacy Impact Assessments and ensure appropriate policies are in place.

Next steps: Consider whether you need to appoint a DPO and, if so, how soon you should be aiming to have someone in that post prior to the GDPR coming into force.

4. Consent rules

Consent to processing of personal data must be freely given, specific, informed, unambiguous and displayed by a statement or by a clear affirmative action. Individuals have the right to withdraw consent at any time.

Next steps: Think about the extent to which you rely on consent to justify your processing of personal data. Will the way in which you obtain consent have to change?

5. Transfers out of the EEA

Parallel legal developments to the GDPR have made this a very hot topic. The old 'Safe Harbor' scheme is no longer effective to transfer personal data to the USA and has been replaced by a new EU/US 'Privacy Shield'.

Next steps: Consider whether you transfer data outside the EEA (especially to the USA). Do you use any cloud services for example? Have you ensured that there is 'adequate protection' for the data being transferred?

6. Subject access requests

The rules governing subject access requests will change. You will not be able to charge for complying with a request and will have a month to comply rather than the current 40 days.

Next steps: Are you comfortable dealing with subject access requests? Do you know what you have to disclose and what you can withhold?

7. Data portability

A new concept of data portability has been introduced. This will enable data subjects to transfer their personal data in a commonly-used electronic format from one data controller to another, enabling people to switch between service providers more easily.

Next steps: Do you have systems in place to cope with this?

8. Right to be forgotten

An individual can require that their personal data is erased if it is no longer necessary, if consent is withdrawn and on grounds relating to the individual's 'particular situation'.

Next steps: Consider whether this may affect your business. Do you have systems and procedures in place to deal appropriately with such requests?

9. Breach notification

The GDPR imposes a mandatory breach notification scheme. Breaches (accidental or unlawful loss, alteration or unauthorised access to personal data) will have to be reported to the ICO within 72 hours. You may also have to report to the individuals whose data has been compromised.

Next steps: You should ensure you have the right procedures in place to detect, report and investigate a personal data breach. Do your agreements with suppliers require them to tell you immediately if there has been a breach? How will you cope with the media and reputational issues?

10. Fines

A two-tiered sanctions regime will apply. Certain breaches will attract a fine of €10m or 2% of global annual turnover, whichever is greater. Fines for more serious breaches will be as much as €20m or 4% of global annual turnover. The ICO can also impose a total ban on data processing by the organisation found to be in breach of its obligations.

We'd be happy to advise you on how the GDPR and other developments in data protection will impact your business and to assist you with putting in place any necessary changes. We can also provide training for your staff at your offices.

Contact our team for more information on how we can help:

Robert Lands
Partner: Head of Intellectual Property
T: +44 (0)20 3755 5557
E: robert.lands@howardkennedy.com

Elizabeth Morley
Senior Associate: Dispute Resolution
T: +44 (0)20 3755 5620
E: elizabeth.morley@howardkennedy.com

Alexandra Johnstone
Solicitor: Intellectual Property
T: +44 (0)20 3755 5827
E: alexandra.johnstone@howardkennedy.com

Susie Al-Qassab
Senior Associate: Employment
T: +44 (0)20 3755 5357
E: susie.al-qassab@howardkennedy.com

No.1 London Bridge
London SE1 9BG
+44 (0)20 3755 6000
howardkennedy.com

howard kennedy