The clock is ticking…

The General Data Protection Regulation (GDPR) will apply in full from 25 May 2018.

The GDPR will significantly change and update the data protection regime across the EU. Every business which handles personal data will need to take steps to adapt and comply with the new regime. Taking action now will minimise the risk of the (increased) GDPR sanctions for non-compliance and reputational exposure and ensure you have sufficient time for any implementation activities.

With less than a year to go, the checklist and suggestions below are designed to help you benchmark the progress of your GDPR project.

---

**Checklist for compliance**

- **Awareness**
  - Have you held kick-off meetings with key stakeholders within the business?
  - Have you identified the key people who will need to be involved in achieving GDPR compliance?
  - Are your staff aware of the GDPR, and that current processes and systems may need to change to comply?

- **Planning**
  - Have you prepared a detailed “roadmap” for compliance with clear roles, responsibilities, goals and actions?

- **Audit**
  - Do you have a good understanding of: the personal data you hold, where it came from, and with whom you share it?

  Key facts to establish include:
  - the types of personal data you hold, and the categories of individuals (data subjects) to whom it relates;
  - which entity is responsible for each category of data;
  - the types of processing undertaken;
  - the purposes for which you have personal data;
  - who the data is shared with (including outside the EEA); and for how long the data is kept.

- **Policies and procedures**
  - Do you already have data processing policies and procedures in place, including a data privacy notice and an internal data protection policy?
  - If so, these should help achieve GDPR compliance, but they will need updating. If not, they are likely to need creating.
  - In essence, they are one (easy) means of meeting enhanced GDPR requirements around transparency and accountability.

- **Basis for processing**
  - What legal basis do you currently rely upon to process personal data?
  - Consider how you currently justify the processing of personal data and whether this is GDPR compliant. In particular, if you rely on an individual’s consent, then assess how you seek and obtain consent as the GDPR contains stricter requirements.

- **Data processors**
  - Do you use data processors to process personal data on your behalf?
  - The GDPR imposes specific, stricter requirements on data processing agreements.
  - If so, are your agreements compliant?

  Check your existing agreements with data processors to see whether they are compliant and, if not, consider what amendments may be needed to meet GDPR requirements.

  When entering into new agreements before May 2018, aim to make them compliant from the start.

- **Pseudonymisation**
  - Do you use data processors to process personal data on your behalf?
  - Are you a data processor?

  If so, then you will become directly responsible for compliance with various GDPR obligations, including: restrictions on sub-contracting processing activities; maintaining records of your processing; data security; appointment of a data protection officer where applicable; transfers of personal data out of the EU and any non-compliance with the data controller’s instructions.

- **Accountability**
  - Do you have a proposed approach to accountability?

  The GDPR requires you to put in place measures to ensure and demonstrate compliance.

  This is likely to require a combination of technology tools, training, staff awareness and policy documentation, supplemented by appropriate records.

  You will need to be able to tell a good compliance story!

- **Privacy by design**
  - Have you implemented the principles of data protection by design and data protection by default?

  This is about embedding the GDPR’s privacy principles in your business. Relevant measures may include: data minimisation; pseudonymisation; transparency of processing; implementing new processes and monitoring these on an on-going basis.

- **Privacy impact assessments**
  - Are you familiar with the guidance on privacy impact assessment and when to use them?

  Privacy impact assessments are a key way of demonstrating a privacy by design approach. It will allow you to identity and correct any privacy issues at an early stage of a project.

  These are not as complex as they sound, but need to be embedded in ways of working where new uses of personal data are being considered.

- **Data protection function**
  - Have you considered whether you need to appoint a data protection officer (DPO)?

  The GDPR requires organisations undertaking certain processing activities in relation to personal data to appoint a DPO. It’s worth considering whether one is required, and if so, whether the right person would be, so they can be involved in GDPR compliance decisions.

  Have you set up your internal data protection function, and determined how management, DPO, relevant employees and other stakeholders will interact?

- **Security and data breaches**
  - Are you able to comply with GDPR’s mandatory breach notification requirements?

  You must notify the relevant supervisory authority of any personal data breach which is likely to result in a risk to the rights and freedoms of individuals within 72 hours of becoming aware of it.

  If the breach is likely to result in a high risk to the rights and freedoms of individuals, then you must also notify those individuals without undue delay.

- **Enhanced rights of individuals**
  - Are you familiar with the enhanced rights of individuals in respect of their data, and are you able to handle requests in time?

  Under the GDPR, individuals have more rights, such as the right:
  - to be informed of processing, or access to data; of rectification of errors; to ensure of data; to restrict processing; to portability of data; and to object to processing.

  Requests must be fulfilled within 30 days.

- **Audit**
  - Have you implemented measures to ensure an appropriate level of security for personal data?

  The level of security should be appropriate to the risk. Suggested measures include: pseudonymisation; encryption; ensuring the integrity, availability and resilience of your systems; being able to restore availability and access to data in the event of an incident; and regular testing of the measures in place.

- **Enhanced rights of individuals**
  - Are you able to comply with GDPR’s mandatory breach notification requirements?

  You must notify the relevant supervisory authority of any personal data breach which is likely to result in a risk to the rights and freedoms of individuals within 72 hours of becoming aware of it.

  If the breach is likely to result in a high risk to the rights and freedoms of individuals, then you must also notify those individuals without undue delay.

---

**Remember**

The approach required will vary between businesses. While GDPR compliance can be complex, we take a business-focused and pragmatic approach to help clients to cut through the jargon, determine what really matters for your business, and devise practical solutions to reduce risk. There are often a number of “quick wins” for businesses who are not where they would like to be at this point in time.

Our data protection team is actively engaged in helping clients get ready for GDPR, and can support you with any of the items raised above. We are also offering clients fixed price one-to-one workshops to help you get GDPR ready.

If you want to find out more about the GDPR and how we can help, please get in touch with one of our data protection team.
Key contacts

Belgium:
- Ann-Sophie De Graeve
  Counsel
  T +32 2 515 9330
  annsophie.degraeve@osborneclarke.com
- Benjamin Docquir
  Partner
  T +32 2 515 9336
  benjamin.docquir@osborneclarke.com

France:
- Beatrice Delmas-Linel
  Managing Partner
  T +33 1 84 82 45 28
  beatrice.delmas-linel@osborneclarke.com
- Claire Bouchenard
  Partner
  T +33 1 84 82 45 30
  claire.bouchenard@osborneclarke.com

Germany:
- Ulrich Baumgartner
  Partner
  T +49 89 5434 8078
  ulrich.baumgartner@osborneclarke.com
- Flemming Moos
  Partner
  T +49 40 55436 4052
  flemming.moos@osborneclarke.com
- Marc Störing
  Partner
  T +49 221 5108 4266
  marc.stoering@osborneclarke.com

Italy:
- Edoardo Tedeschi
  Partner
  T +39 02 5413 1757
  edoardo.tedeschi@osborneclarke.com

The Netherlands:
- Jeroen Lub
  Partner
  T +31 20 702 8616
  jeroen.lub@osborneclarke.com

Spain:
- Rafael Garcia Del Poyo
  Partner
  T +34 91 576 44 76
  rafael.garcia@osborneclarke.com

UK:
- Mark Taylor
  Partner
  T +44 20 7105 7640
  mark.taylor@osborneclarke.com
- Will Robertson
  Partner
  T +44 117 917 3660
  will.robertson@osborneclarke.com
- Ashley Hurst
  Partner
  T +44 207 105 7302
  ashley.hurst@osborneclarke.com
- Nick Johnson
  Partner
  T +44 20 7105 7080
  nick.johnson@osborneclarke.com

US (West Coast):
- Emily Jones
  Partner
  T +1 650 462 4028
  emily.jones@osborneclarke.com

US (East Coast):
- Steve Wilson
  Partner
  T +1 917 545 3672
  steve.wilson@osborneclarke.com

Where we work

Belgium: Brussels
China: Shanghai
France: Paris
Germany: Berlin, Cologne, Hamburg, Munich
Hong Kong
India: Mumbai*
Italy: Milan, Brescia, Padua, Rome, Busto Arsizio
The Netherlands: Amsterdam
Singapore
Spain: Barcelona, Madrid, Zaragoza
UK: London, Bristol, Thames Valley
USA: Silicon Valley, New York, San Francisco

Osborne Clarke is the business name for an international legal practice and its associated businesses. Full details here: osborneclarke.com/definitions

* Relationship firm

osborneclarke.com