MAYER·BROWN

Legal Update
February 2017

Preparing to comply with The EU General Data Protection Regulation

The new European General Data Protection Regulation (GDPR) will come into force throughout the European Union on 25 May 2018. The GDPR will replace existing data protection laws throughout Europe and introduce significant changes and additional requirements that will have a wide ranging impact on businesses around the world, irrespective of where they operate.

The GDPR: The changes that will affect your business

The key changes and additional requirements introduced by the GDPR are:

1. **European data protection law will now apply worldwide.** In a significant departure from the current requirements, in addition to businesses that are established in the European Union, organisations that are located outside the EU that process personal data in relation to the offer of goods or services to individuals within the EU, or as a result of monitoring individuals within the EU, will have to comply with European data protection law. Non-EU based businesses will need to consider whether they will be subject to the new rules and how they will comply.

2. **Tougher sanctions for non-compliance.** The maximum fine for a breach of European data protection law will be substantially increased to 4% of an enterprise's worldwide turnover or €20 million per infringement, whichever is higher.

3. **A new data breach notification obligation.** Organisations will now have to notify the relevant European data protection authority of a breach without undue delay and where feasible within 72 hours. A notification must also be made to the individuals affected without undue delay where there is a high risk to the individuals concerned.

4. **New data privacy governance, data mapping and impact assessment requirements.** Organisations will now need to appoint a data protection officer to be responsible for implementing and monitoring that organisation's compliance with the GDPR and to carry out assessments of an organisation's data processing in certain circumstances. Organisations will now also be required to map their processing of personal data and undertake data protection impact assessments for higher risk processing.

5. **A requirement to implement 'privacy by design'.** Businesses must now take a proactive approach to ensure that an appropriate standard of data protection is the default position taken when personal data is being processed.

6. **Strengthening of individuals' rights to personal data.** Individuals will have the right to have their personal data removed from systems or online content (the 'right to be forgotten'), the right not to be subjected to automated data profiling (where this would produce a legal effect), and the right to be given a copy of the personal data relating to them in a commonly used format and to have that information transmitted to another party (the 'right to data portability'). Organisations must determine how they will enable individuals to exercise these rights.

7. **Enhanced requirements for the supply chain.** Businesses must only use other parties to process personal data that provide sufficient guarantees that they will implement appropriate security measures to satisfy the requirements of the GDPR. These service providers will now be held accountable for their own level of appropriate security, must document their processing to the same extent under the GDPR and must obtain prior consent to employ sub-processors. Organisations will need to review and amend their contracts with these parties to address the changes in responsibilities.

Preparing for the GDPR: The 10 steps your business should take to get ready to comply

If a preliminary assessment determines that your business will have to comply with the GDPR, your business should take the following 10 key steps:

1. **Inform your leadership and formulate a plan.** Senior management should be made aware of the changes to data protection law and how it will affect your business. Senior management should designate the individuals that will formulate a plan for how your business will implement the requirements of the GDPR and will educate the wider workforce on its operational impact.

2. **Appoint a data protection officer.** A decision should be made as to whether it is required under the GDPR or otherwise desirable for your organisation to appoint a data protection officer who will be responsible for the implementation of the requirements of the GDPR and monitoring compliance with it. This person should act as the head of your data protection governance structure, report directly to leadership and should be responsible for putting controls in place to implement and monitor compliance.

3. **Map your personal data.** A detailed investigation should be conducted into and a record created of the personal data your business is collecting, the purposes for which it is being processed, how it was obtained and the parties that it is being shared with.

4. **Examine the impact.** The information gathered from the personal data mapping exercise should be used to assess which parts of your business and which data processing activities must comply with the GDPR.

5. **Address the risks.** Data protection impact assessments should be conducted to identify and minimise the risks associated with the processing of personal data by your business, particularly where there are high risks to the rights and freedoms of the individuals concerned by the activities that are being or are going to be carried out.

6. **Review the grounds under which personal data is being processed.** How and the basis under which personal data is being collected and processed should be reviewed to determine if any changes need to be made for this to continue under the GDPR, particularly where 'consent' and 'legitimate interests' (which are more difficult to demonstrate under the GDPR) are being relied upon to process personal data.

7. **Update your data governance.** Policies, procedures and other governance controls within your business should be updated to detail how your organisation will practically comply with the new requirements under the GDPR. Employees should receive training on and should be regularly updated about this.

8. **Implement new compliance systems.** Plans and mechanisms must be put in place to ensure that the business can respond to a data breach and the new data breach notification requirements, the rights to be forgotten, to data portability, to object to automated data profiling, to be provided with access to personal data and other rights that individuals can exercise in relation to their personal data.

9. **Review your supply chain contracts.** The contracts with the service providers and other parties that your business shares personal data with should be reviewed and, where necessary, renegotiated to ensure that your organisation is appropriately supervising the manner in which they process personal data and that those parties are complying with their obligations under the GDPR.

10. **Assess your international transfers.** Assess the manner in which you currently carry out any international transfers of personal data and whether any mechanisms for carrying out these transfers within your organisation or to third parties needs to be updated to comply with the European data protection requirements.

The GDPR and the Mayer Brown GDPR Readiness Service: Key contacts

For more information about the GDPR and the Mayer Brown GDPR Readiness Service, please contact any of the following:

EUROPE, MIDDLE EAST, AFRICA

Charles-Albert Helleputte
Partner, Brussels
chelleputte@mayerbrown.com
+32 2 551 5982

Dr Guido Zeppenfeld
Partner, Frankfurt/Düsseldorf
gzeppenfeld@mayerbrown.com
+49 69 7941 1701/+49 69 7941 1701

Mark Prinsley
Partner, London
mprinsley@mayerbrown.com
+44 20 3130 3900

Oliver Yaros
Partner, London
oyaros@mayerbrown.com
+44 20 3130 3698

AMERICAS

Rebecca Eisner
Partner, Chicago
reisner@mayerbrown.com
+1 312 701 8577

Lei Shen
Senior Associate, Chicago
lshen@mayerbrown.com
+1 312 701 8852

Rajesh De
Partner, Washington DC
rde@mayerbrown.com
+1 202 263 3366

David Simon
Partner, Washington DC
dsimon@mayerbrown.com
+1 202 263 3388

Kendall Burman
Counsel, Washington DC
kburman@mayerbrown.com
+1 202 263 3210

ASIA PACIFIC

Gabriela Kennedy
Partner, Hong Kong
gabriela.kennedy@mayerbrownjsm.com
+852 2843 2380

0408ipt