A new era approaches for European data protection

January 2016

On 15 December, the EU Parliament and the Council of the European Union reached provisional agreement on the new European General Data Protection Regulation (the ‘GDPR’). Although the core principles of the current regime have been retained, the GDPR will introduce new obligations and higher sanctions, and for many organisations will require a culture shift in their approach to handling and using personal data. The GDPR also has wide extra-territorial reach and as a result will be relevant to a larger number of non-EU based companies than the current regime.

The Council and the EU Parliament still need to formally approve the GDPR, which they expect to do in spring this year. The GDPR will be directly applicable in all Member States two years after its formal adoption. Although two years may seem a long time, for a number of organisations there is much to achieve in that period. Preparing for the GDPR now will make the end of 2017 and the beginning of 2018 much less painful.

This briefing is the first in a series of publications that we will publish on the GDPR. It sets out practical steps that companies should consider taking now. Subsequent publications will look at the implications for companies of some of the specific changes the GDPR will introduce.

Practical Steps

Step 1
Assess whether the GDPR will apply to your organisation

- If your organisation is a non-EU based company, does it provide goods or services (including free of charge) to individuals in the EU (e.g. a website in a European language targeting those markets)? Do you monitor the behaviour of individuals that takes place in the EU? If so, the GDPR will apply to you.
- The GDPR will be relevant to your organisation if it is a controller but also if it is a processor. For the first time, processors will have direct obligations imposed on them by law (e.g. maintaining records and putting in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk).

Step 2
Board buy-in

Assessing the impact of the GDPR and the preparation of a plan to implement any necessary changes can be expected to require additional resources and support from various parts of the organisation. Early board buy in may assist with both of these. Reasons to put forward as to why the board should support the additional resource include:

- Risk - Current impact/likelihood risk assessments in relation to data protection compliance will need to be revised. The introduction of stronger sanctions, including maximum fines of up to 4% of annual worldwide turnover or 20,000,000 Euros, whichever is the highest, will be relevant in this regard.
- Reputation and competitive edge - For consumer based organisations, careful planning in advance can help ensure the customer journey is not unduly affected. Transparency, trust and handing control back to the individual are likely to be key components of an effective compliance strategy.
Step 3
Audit - understand how your business uses personal data

- What data is collected? Is it sensitive personal data? What are the data flows?
- Is there any anonymised data that could become personal data? The definition of personal data in the GDPR is wider than under the current regime.

Step 4
Assess current compliance levels

Much of what was best practice is now law (e.g. privacy by design, data security breach notification, maintaining detailed records of processing and policies and procedures and appointment of data protection officer). If your organisation was already complying with best practice, it will have a head start.

Step 5
Carry out a gap analysis and identify key areas of risk for your business

- Does your organisation carry out profiling (or data analytics)? In some circumstances profiling will need the explicit consent of the individuals concerned.
- How much information does your organisation provide to individuals about how their data is used? The GDPR contains a more comprehensive list of items of information to communicate.
- Does it regularly use data processors (including overseas ones) or has it outsourced a part of its business (including personal data of customers or employees)? The direct obligations placed on processors in the GDPR may result in a shift in processors’ attitude to risk.
- Does your organisation have systems and processes in place for dealing with data security breaches? Organisations will have to notify the regulator (and individuals in some cases as well) of data breaches without undue delay and, where feasible, within 72 hours unless the breach is unlikely to be a risk to the rights and freedoms of individuals.
- To what extent does your organisation ensure that privacy risks are considered at the outset of a new project (privacy by design)? Controllers will be required to carry out data protection impact assessments (DPIAs) where the processing operations are likely to result in a high risk for the rights and freedoms of individuals. DPIAs are useful in a number of situations, including to help with understanding the impact of the gap analysis on your business.
Conclusion

There is no need to rush into immediately changing policies, procedures and behaviours. Parts of the GDPR are still unclear or require further clarification, including the passing of national legislation to flesh out specific rules (e.g. in the context of employment and prevention of criminal offences). National data protection authorities, the European Data Protection Board (which replaces the Article 29 Working Party) and other sector bodies will also be publishing guidance, all of which we will be closely monitoring.

The ICO has also acknowledged that it will take time to understand fully all the implications of the new legislation. However, the importance of the GDPR cannot be understated. In order to future proof current activities and to ensure an orderly transition, organisations should be taking the steps outlined above now, to the extent they are not already doing so.