ALLEN & OVERY

Preparing for GDPR compliance

The General Data Protection Regulation is transforming privacy and data protection in the European Union. With little time left to achieve compliance and severe sanctions looming over those that fail to do so, practical measures need to be taken now.

The European Union's (EU) General Data Protection Regulation (GDPR), which applies from 25 May 2018, has triggered a sea change in privacy and data protection. Virtually any organisation that has a physical presence in the EU, as well as many that are not established there, are likely to be caught by the new rules. Those that fail to comply face potentially severe sanctions including fines that could, in some circumstances, reach up to 4% of annual global turnover.

The scale and complexity of the GDPR should not be underestimated. Simply relying on past practice or extending current procedure is unlikely to deliver the required level of change. Many organisations will often be better off taking a 'blank sheet of paper' approach to compliance to ensure there is a robust reworking of data protection practices. The magnitude of such an undertaking, however, is likely to place a substantial burden on internal teams working on GDPR implementation programmes.

Achieving compliance has therefore become one of the most pressing risk management challenges facing senior management and boards of directors.

With relatively little time left until the GDPR comes into force, general counsel and in-house legal and compliance departments should focus their efforts on identifying and prioritising the most significant changes that must be put in place by 25 May 2018.

Allen & Overy has published a practical guide to GDPR. To request your copy of *Preparing for the General Data Protection Regulation (January 2018)*, email bastian.renner@allenovery.com

In our view, there are a number of high risk areas that organisations should look to address urgently.

Widening scope

Although much of the GDPR represents the codification of existing good practice, there are a number of new rules that organisations will have to address. Defining territorial reach – the scope of application of the GDPR to cross-border business activities – is perhaps one of the most challenging of these changes.

Under the GDPR, multinational businesses will be subject to the scope of its requirements in a wider range of circumstances than ever before. The GDPR applies to an organisation if it is established in the EU and processes data anywhere in the context of that establishment.

Eight things you should be doing now to prepare

1. Prepare for data security breaches
2. Establish a framework for accountability
3. Embrace privacy by design
4. Analyse the legal basis on which you use personal data
5. Check your privacy notices and policies
6. Bear in mind the rights of data subjects
7. If you are a supplier to others, consider whether you have new obligations as a processor
8. Cross-border data transfers – it is important to ensure that you have a legitimate basis for transferring personal data to jurisdictions that are not recognised as having adequate data protection regulation.

But even if an organisation is not established in the EU at all, the GDPR will apply if it offers goods or services to, or monitors the behaviour of, individuals who are located in the EU.

When it comes to websites, certain factors will be more likely to bring non-EU organisations into the reach of the GDPR. While there is no need to take a blanket approach and block EU users from websites targeted at a non-EU audience, it is important to take a very close look at content and language. For instance, an activity is likely to come within the scope of GDPR, if a company is providing goods or services from the United States but the language is adapted to EU countries. Another trigger for application of the GDPR might be the provision of access to local support (for example, a helpdesk) alongside a website.

Consent – when is it needed?

Relying on consent as a basis for processing data will become much more difficult under the GDPR. Consent must be given freely and be specific, informed and unambiguous. It must never be a pre-condition of performing a contract or the provision of a service. It should not be hidden away in terms and conditions and it must be as easy to withdraw as to give consent. There are various other legal bases for processing data that may be available. An organisation may, for example, be able to rely on legitimate business interests as grounds to process data in a wide array of circumstances.

The GDPR provides that companies can continue to rely on a variety of techniques to obtain consent, but using pre-ticked boxes is prohibited. Should an organisation intend to use a consent obtained previously as a basis for new processing of data, the organisation will need to go back to the data subject and seek further consent.

Increased transparency

The design, wording and the information contained in privacy notices require very careful attention.

Individual data subjects must have information made available to them about the manner in which, and the purpose for which, their personal data is processed. That information must be concise, transparent, intelligible and easily accessible. At the same time, the list of information that must be included in a privacy notice has expanded significantly.

This poses a fundamental challenge in designing privacy notices. On the one hand, the data controller must communicate with the individual in a clear and intelligible manner, but, on the other hand, it must communicate quite detailed and forward-looking information about its data processing activities.

Legal and compliance teams should review privacy notices to ensure all required information is included. Notices should also be reviewed for readability and comprehensibility.

Frequently asked questions about the impact of Brexit on GDPR

Is Brexit an 'escape route' for UK-based organisations?

No. Until Brexit negotiations are concluded, the UK is still part of the EU and therefore will be subject to the GDPR from 25 May 2018. The UK government has stated that it is keen to align domestic law with the GDPR and its proposed Bill, which executes its derogations and exemptions under the GDPR, is currently being looked at by the House of Commons.

What will happen when the Brexit deal has been decided?

As things stand, it looks likely that the UK will become a 'third' country for the purposes of cross-border data transfers. Unless some form of 'adequacy' decision is immediately made (which doesn't look likely), other steps will need to be taken to move data to the UK from the EU. The UK government therefore favours a transition period of mutual recognition followed by some form of enhanced adequacy regime.

Consideration should be given to how privacy notices are communicated. One option may be to consider layering of privacy notices, so as to draw only unexpected or otherwise key information to the individual's attention, while allowing them to find further details, should they wish to do so.

Expansion of rights

One of the cornerstones of the GDPR is to strengthen the rights of individual data subjects, such as the right of a person to access information about the data being processed about themselves, the 'right to be forgotten' and the right to data portability.

Implementing these expanded and strengthened rights could pose a significant operational challenge. Organisations that receive more than a handful of requests will need a robust process for responding, given that information must be provided free of charge and within a month of receiving a request.

It is feared by some that the removal of the right to charge a fee for responding to access requests could lead to a sharp increase in the volume of certain types of requests. This is an area that requires careful attention as regulators are set to take a tough line with organisations on these sorts of requests (particularly, as they are frequently a cause of complaints by individuals). Regulators are also likely to press organisations to adopt more robust processes to the extent that they fall short.

Accountability and privacy by design

Another critically important element of the GDPR is the enhanced level of accountability that it places on data controllers to demonstrate compliance. As part of this new accountability regime, organisations will need to maintain detailed records of all processing activities. Although such a requirement is likely to be an onerous task, it can also be a useful practice, enabling an organisation to fulfil other obligations more efficiently and at the same time highlight areas where compliance is not sufficiently thorough.

In parallel, data controllers will also have to conduct regular data protection impact assessments (DPIAs) for high risk processing, and ensure privacy by design. It is essential that data controllers are aware when DPIAs are necessary and that they are recorded.

Moreover, appointing a data protection officer (DPO), where required, could represent a significant change. DPOs should have expert knowledge and report to the highest level of management. Many companies are looking to appoint internally by identifying an employee with some privacy knowledge and providing them with appropriate training.

Data breaches

Loss of, or unauthorised access to personal data, must be treated extremely seriously. Obligations to notify regulators and affected individuals will apply in many cases, and are expected in very short timescales.

Data processors have an obligation to notify controllers without delay. Data controllers must notify supervisory authorities within 72 hours of awareness, where feasible, unless the breach is unlikely to pose a risk to individuals. Data controllers may also need to notify the data subject in certain circumstances.

What is privacy by design?

Privacy by design is an approach to protecting privacy in the creation of systems (technologies, business practices and physical design of networked infrastructures) that focuses on privacy upfront by embedding it into the architecture from the beginning.

Privacy by design means implementing appropriate measures both when determining the means for processing and at the time of the processing itself, which implement the data protection principles (such as data minimisation). When thinking about privacy by design, an organisation should take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks to individuals.

This obligation requires considering privacy at the beginning of undertaking new activities involving personal data processing, or when implementing new or modified data management systems.

Given that the timeframes to notify a breach are so short, having a strategy in place is vital. Regulators regard notification as important because it enables them to prepare for any public fallout. Aside from the legal implications of the situation, a degree of courtesy with regulators can also help to foster a healthy relationship.

Compliance challenge

Implementing the GDPR has the potential to be costly, time-consuming and disruptive, but it should certainly be a realistic goal for those willing to plan and prioritise high risk areas effectively and commit the necessary resources to achieve compliance.

As David Smith, former deputy commissioner at the UK Information Commissioner's Office (ICO), who is now a special adviser to Allen & Overy, explains in the foreword to our latest publication, *Preparing for the General Data Protection Regulation (January 2018)*: "Getting data protection right is not just a matter of legal compliance. It also makes sound business sense."

Contributors

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Nigel Parker
Partner – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Charlotte Mullarkey
PSL Counsel
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com

David Smith
Peerpoint Consultant
Tel +44 20 3088 6842
david.a.smith@allenovery.com