European General Data Protection Regulation finally adopted: are you ready?

Data Protection Alert

Data Protection, Privacy and Security Alert

14 APR 2016

Today, 14 April 2016, the EU Parliament adopted the long awaited General Data Protection Regulation (GDPR). The Regulation will have a considerable impact on all organisations based in the European Union that process personal data, but also on organisations based outside of Europe providing services to the European market.

The GDPR is expected to be published in the Official Journal of the European Union by June, and 20 days after publication the GDPR will enter into force. **From that moment onwards, the clock starts running:** companies will have two years to prepare themselves to comply with the GDPR.

Key changes

The GDPR replaces the current European data protection regime consisting of the 1995 Data Protection Directive and 28 national data protection laws. The GDPR will be directly applicable in every EU member state, without the necessity of national implementing laws.

The Regulation contains many key changes, such as:

1. **Harmonisation**: There will be a single set of rules on data protection, directly applicable in all EU member

states, thereby mitigating the current fragmentation of national data protection laws.

2. **Stronger enforcement**: Non-compliance could lead to heavier sanctions. The revised enforcement regime is underpinned by power for regulators to levy financial sanctions of up to 4 percent of the annual worldwide turnover of the organisation.

3. **Offshore processing**: The GDPR will apply to companies established outside the EU that process data related to the activities of EU organisations. Non-EU companies will also be subject to the Regulation if they target EU residents by profiling, or proposing products or services.

4. **Governance**: Organisations will have increased responsibility and accountability on how they control and process personal data.

5. **Consent**: The Regulation requires a more active consent based model to support lawful processing of personal data; wherever consent is required for data to be processed, consent must be explicit, rather than implied.

6. **Transparency**: Organisations will have increased transparency obligations; privacy notices will need to include much more detailed information.

7. **Data breaches**: Organisations will be required to notify the local supervisory authority, and (in some cases) data subjects, of significant data breaches.

8. **Data portability**: Organisations must ensure data subjects can easily transfer their data files from one service provider to another.

9. **Right to be forgotten**: The GDPR consecrates the "right to be forgotten", allowing data subjects the right to require a controller to delete data files relating to them if there are no legitimate grounds for retaining it.

10. **Data processors**: Organisations processing data on behalf of other companies will be required to comply with a number of specific data protection related obligations. They will be liable to sanctions if they fail to meet these criteria.

11. **Data Protection Officer**: Companies will have to appoint a Data Protection Officer when they are, for example, processing sensitive data. The DPO will report to the highest management level.

12. **One-stop-shop**: A single national data protection authority will act as the lead regulator for compliance issues in the EU, where the organisation has multiple points of presence across the EU.

13. **Privacy impact assessment**: A PIA will become a mandatory prerequisite before processing personal data for operations that are likely to present higher privacy risks to data subjects due to the nature or scope of the processing operation.

14. **Privacy by design and privacy by default**: Companies must take privacy risk into account throughout the process of designing a new product or service, and adopt mechanisms to ensure that, by default, minimal personal data is collected, used and retained. An approved certification mechanism can be used to demonstrate compliance with the applicable requirements.

It should be noted that the 2002 E-Privacy Directive regulating cookies and spam remains in place and is currently under review. Organisations should continue to follow national rules on cookies and spam.

Join one of our "GDPR - Are You Ready?" events

Across the world, as well as online, we are planning events in 30 locations throughout 2016 and 2017 in the form of seminars, roundtables and workshops on how to get ready for GDPR compliance. Information about these events will be coming soon.

Are you ready?

The implementation phase has started: You will have two years to ensure your data processing activities are in line with the newly adopted rules. This means needing to act now.

It makes sense to undertake a snapshot assessment of the impact of the Regulation on the business, so that steps can be taken to identify and implement any necessary changes. Any assessment ought to be tailored to the specific needs of the business but is likely to focus on key issues such as fair processing, privacy notices, information governance, privacy impact assessments, appointment of a DPO, data breach procedures, and data transfers.

National data protection authorities, as well as the European privacy bodies, will be issuing guidelines and opinions in the next months to assist organisations in their preparation.

We are ready

We are ready to support you. Our DLA Piper Global Data Protection, Privacy and Security team of more than 130 data protection lawyers around the globe provide assistance on all aspects of privacy compliance related legal support, implementing practical risk based solutions that align to the way your business operates, where possible turning privacy compliance into a competitive advantage. Our global presence combined with our depth of experience in each region gives you the important advantage of local knowledge and cultural awareness, combined with consistent, practical advice.

Our experience includes:

- Assisting organisations in preparing for the Regulation and development of effective organisational controls and governance structures
- Carrying out a privacy impact assessment for your organisation to evaluate the nature and sensitivity of the data processing operations you currently carry out or envisage carrying out in the future
- Managing data security breaches
- Advising on supply chain and cross-border data issues
- Liaison with regulators
- Defending class action privacy lawsuits
- Advising on how to maximise value from data assets consistent with the regulatory landscape
- Monitoring regulatory developments and providing practical impact assessments
- Supporting privacy by design in new projects

Within our practice, we have developed a comprehensive set of tools to support development of each component part of the information governance framework.

Next steps

For further information please visit our dedicated GDPR microsite.

If you would like to discuss how we can help your organisation prepare, please get in touch with your usual DLA Piper contact or email us at .