On 25 January 2012, the European Commission outlined its proposals for a radical overhaul of data protection rules in the European Union. The proposed law will increase compliance obligations of companies with the possibility of the imposition of fines of up to 2% of global turnover of the offender.

With these new rules the Commission aims to develop a more coherent and unified data protection law throughout the EU.

The new data protection law is expected to be enacted by a regulation, which will supersede the existing Data Protection Directive (95/46/EC). Unlike directives, regulations do not require any implementing measures at local member state level. Hence they become immediately enforceable as law in all member states simultaneously. According to the draft text, "(the) direct applicability of a Regulation...will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules...". In other words, adopting these reforms by regulation means that member states have no scope to pass diverging domestic laws.

It is expected that the changes will be in force before 2015.

We have highlighted below some key issues that you should be aware of in order to prepare for compliance with the Regulation.

Data Protection Representative in the EU
Where a business is based outside of the EU but it offers goods or services for sale to, or monitors the behaviour, of consumers in the EU, then that business must have a nominated representative based in the EU. A business that fails to appoint an EU-based representative could face fines of up to 2% of its global turnover.

Notification of Breach
Where a data protection breach occurs, the business involved will have to notify the regulator in all cases and the affected individuals, where there is a chance that there will be an adverse affect to that person's privacy. The business will not be obliged to advise the individuals of the breach where the data has been protected with software to the extent that it renders the data unintelligible to any person who is not authorised to access it. Failure to comply with security
obligations and breach notification requirements could result in fines of 2% of the global turnover of the company. This is an important change and effectively places the key principles of the Irish Data Protection Commissioner’s Data Breach Code of Practice on to a statutory footing.

Data Protection Officer
Public authorities, businesses employing more than 250 people and companies where the core activities consist of processing activities (which regularly and systematically monitor data subjects) must have a designated “Data Protection Officer”. Groups of undertakings can appoint a single Data Protection Officer to represent them. Individuals can contact the Data Protection Officer in relation to all issues regarding their data and in exercising their rights under the Regulation. A fine of 2% of its global turnover applies should a Data Protection Officer fail to be appointed.

New Fundamental Principles
In addition to the existing data protection principles, (for example, that processing be for “limited purpose”, be “not excessive” and “relevance”, etc.) several new principles have been introduced.

» Every individual has the right not to be profiled and profiling can only occur where special circumstances are met.

» Where processing of information presents specific risks to the rights and freedoms of individuals due to their nature, scope or purpose, then the data controller must undertake a data protection impact assessment and obtain prior authorisation from the supervisory authority before the processing takes place.

» The Regulation has also introduced the somewhat controversial “right to be forgotten”. An individual can simply withdraw their consent to have their data processed and the information held about them must be erased. This right is subject to limited exceptions e.g. a controller will not be compelled to erase the personal data of a data subject in circumstances where it is needed for “historical, statistical or research purposes”.

» Where an individual’s personal data is processed by electronic means and in a structured and commonly used format, it is possible for the data subject to obtain a copy of that data.

Subject Access, Rectification and Erasure
Individuals can continue to make data subject access requests. There is a wider scope of “personal data” and penalties for failure to comply will also arise. For example a late response to an access request could result in a fine of 0.5% of the global turnover of the company.

Commercial Arrangements
Where there is an agreement/arrangement in place (e.g. outsourcing) which involves the processing of personal data, parties are obliged to acknowledge the data protection risks at an early stage. It is necessary to document all processing undertaken by data controllers and data processors. Controllers must also undertake a security evaluation in advance of any processing and take the appropriate security measures to ensure the data remains safe. Furthermore, where there are joint controllers of data, they must assign the risk between the parties. A breach of these new requirements could result in a fine of up to 2% global turnover of the company.

Transparent Policies
It is necessary for each business to ensure that data protection policies are in place and that they are transparent and easily accessible. Article 14 sets out an extensive list of information that must be provided to data subjects including, in addition to the information set out in the current Directive, the period for which the data will be stored, the right to object to the processing of the personal data and the right to lodge a complaint with the supervisory body and the contact details of that body. Failure to adhere to this requirement could result in fines of up to 1% of their global turnover.

Marketing
The meaning of “consent” is amended to mean that it is “any freely given, specific, informed and explicit indication of his or her wishes”. While it is possible to interpret this as a statement or an affirmative act, such as ticking a box, it is not sufficient to use a pre-ticked box or an assumption of consent.

Consequently, it is necessary to ensure that direct marketing campaigns are only aimed at those who have agreed to accept them within the new meaning of “consent”. It is likely that a breach of this aspect of the regulation will result in a fine of up to 2% of the global turnover of the company.

Personal Data of Children
The Regulation is particularly strict in relation to the gathering of personal data from children due to their probable lack of understanding of the gravity of having their personal data collected and processed. This is an area in which the Commission has previously tried to introduce voluntary codes of practice, e.g. with social network sites, albeit with limited success. “Consent” of a child under the age of 13 is only valid if it is given by a parent or guardian of that child. It is important that the data controller makes “reasonable efforts” to obtain verifiable consent from a child, taking into consideration the technology involved. Non-compliance could result in fines of up to 2% of the global turnover of the company.

What do you need to do to comply with this Regulation?

» Nominate a Data Protection Officer within your business.

» If your business is based outside of the EU, plan to appoint a data protection representative who is based within the EU.

» Examine your organisation’s data breach procedures and have a clear plan of action should a data breach occur. Ensure that those responsible for putting the
plan into action know who to notify within the relevant time lines.

» Review your internal data protection policies. Training might be required for your staff to ensure their dealings with personal data are legally compliant.

» Ensure there is a procedure in place for dealing with data access requests in a pro-active, timely and efficient manner.

» In commercial agreements, examine the data protection risks and apportion risk at an early stage between the parties involved.

» Ensure that data protection policies are easily accessible and are transparent to individual data subjects.

» Make certain that the appropriate information relating to the party collecting the data and the purposes for which it is to be used are provided at the earliest possible stage.

» Review all consents received for direct marketing campaigns and ensure they fit within the new definition of “consent”. Change the method that consent is obtained from consumers so that consent is demonstrated by an affirmative action.

» Establish if your organisation processes personal data about children and if it does whether the mechanisms for obtaining consent are sufficient. If it is not satisfactory it will be necessary to change the manner in which you obtain consent.

Contacts
For further information, please contact one of the following Arthur Cox lawyers:

John Menton
Partner, Head of Technology Group
+353 (0)1 618 0558
john.menton@arthurcox.com

Caroline O’Gorman
Associate, Technology Group
+353 (0)1 618 1190
caroline.ogorman@arthurcox.com

Chris Bollard
Associate, Technology Group
+353 (0)1 618 0649
chris.bollard@arthurcox.com

Rob Corbet
Partner, Technology Group
+353 (0)1 618 0566
rob.corbet@arthurcox.com

Colin Rooney
Associate, Technology Group
+353 (0)1 618 0543
colin.rooney@arthurcox.com

Olivia Mullooly
Associate, Technology Group
+353 (0)1 618 1160
olivia.mullooly@arthurcox.com

or your usual Arthur Cox contact.