EU Data Protection Reforms Update

Date : May 19, 2014

What is this all about?

The EU is reforming its existing data protection rules and this article provides a brief update on the main issues and where things currently stand in order to draw attention to their eventual compliance impact, especially because the reforms are more than just an upgrade.

What is EU data protection?

The right to privacy is protected in various ways in the EU. It is essentially regulated under a 1995 EU Directive that controls the processing of personal data, regardless of whether such processing is automated or not.

At its most basic, the core principle is that personal data should not be processed except where certain conditions are met, as set out under the 1995 rules. Here, “personal data” essentially means any information relating to an identified or identifiable natural person, otherwise technically referred to as a “data subject”, i.e an identified or identifiable person to whom specific personal data relates - an identifiable person is one who can be identified, directly or indirectly, by reference to various factors. The “processing of personal data” essentially means any operation or set of operations which is performed upon personal data. The other parties involved in the process are the “data controller”, who is the person or entity determining the purposes and means of the processing of personal data, and, the “data processor”, who is the person or entity processing personal data on behalf of the controller.

Data protection regulators, usually officially referred to as “supervisory authorities” are independent bodies set up in each EU Member State whose task is to enforce data protection regulation, including dealing with complaints and violations.

It is no exaggeration to say that the EU data protection rules have been of very wide effect, not only within the EU but externally as well with major compliance requirements on businesses inside and outside the EU. Of particular note under the reforms is the widened impact on businesses outside the EU.

Why is this happening ?

Some two years ago the European Commission officially began the legislative reform process with as its main objective a significant overhaul of the rules set out under the 1995 EU Directive, in particular in light of the global development of the Internet and information technology. Another important aim is to introduce a less administratively burdensome and costly regime for businesses. Further, it is hoped that enhanced data protection compliance will give businesses a competitive advantage.

Are these completely new rules?

Yes and no: yes, the 1995 rules are being completely replaced; no, the fundamental aspects of privacy are still being protected. The difference will be in the detail as the reforms essentially build on the current structure - if enacted in current form, the 1995 rules will be tripled in length, or, even more depending on the number of amendments on top that are eventually accepted under the EU legislative process.

What types of new rules will there be?

There are in fact two proposed sets of new rules: a Regulation, which sets out a general EU framework for data protection - this will replace the existing 1995 Directive and it is notable that it is in the form of a Regulation as this legislative format will be immediately applicable once adopted, i.e it will not require EU Member States to enact the type of further legislation needed to enact a Directive; and, a Directive, which specifically deals with protecting

personal data processed in a law enforcement context - this Directive is not really of concern to businesses.

Where do things stand?

In March 2014, by plenary vote, the European Parliament approved the amendments made at its committee level. Overall, the Parliament has left the main elements of the Commission's proposal in place and has instead added greater detail.

How many data protection regulators will I have to deal with?

Under the reforms, there will be one set of data protection rules across the entire spread of 28 EU Member States. The upshot of this is that a business which is in several EU Member States should only have to deal with one data protection regulator, which will most likely be in the country where the business is based - the Parliament's proposed amendments have somewhat diluted this notion though.

My business is not in the EU so will these rules still affect me?

The new EU data protection rules will apply not only to businesses which are actually located in an EU Member State, but, also, to businesses located completely outside the EU where these latter businesses process (through their processors/controllers) data of EU residents to whom these businesses offer their goods and services. This extra-territorial dimension is the most significant and at the same time probably the most controversial aspect of the reforms and has been criticized as being difficult if not impossible to effectively enforce.

Will I have to make privacy an integral compliance element in my business ?

Privacy by design and/or default will not be an add-on, but, instead, will become the norm as businesses will have to incorporate data protection safeguards into their products and services from the very start. In its proposed amendments the Parliament goes even further by seeking to ensure an entire lifecycle of personal data management.

Will consent be required consent for data processing?

Explicit consent will have to be given by a data subject in order for his/her data to be processed.

Is there a right to have data deleted?

Where there are no proper grounds for keeping data, a data subject will have the right to have his/her data deleted, subject to provisos about the freedom of expression and information. This is also considered as a controversial aspect of the reforms.

Will data-profiling be allowed?

A data subject will have the right to not to be subject to data-profiling, subject to certain exceptions.

Will I need to appoint a data protection officer?

A special data protection officer will have to be appointed to deal with data protection compliance in certain circumstances, for example, where the processing is carried out by a business which employs 250 people or more, or, where processing operations, require regular and systematic monitoring of data subjects.

When will I have to report data breaches?

Personal data breaches can take several forms and are a form of security breach, which is a serious compliance

issue. Under the reforms, data breaches will have to be reported to data protection regulators without delay and, where possible, not later than a period to be set under the new rules, which is currently set at 24 hours but which in the final version of the reformed rules may be longer - the notification to the regulator will have to be accompanied by a reasoned justification in cases where it is not made within the set period.

What kind of fines can my business face for breaching the rules?

Under the reforms, data protection regulators will have the power to impose fines for infringing the data rules of up to Euro 1 million or up to 2% of the global annual turnover of a business, whichever is the greater, which may well go up in the final version of the reformed rules.

Will some kind of other assessments have to be made?

Where processing operations present specific risks to the rights and freedoms of data subjects, data processors/controllers will have to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, for example, in large-scale filing systems on children.

Has anything changed as regards data transfers to third countries?

The core principles concerning the transfer of data from EU Member States to third countries will remain in place, including the requirement that such data flows can only occur where an adequate level of protection is assured by these third countries. What the reforms mainly introduce is an extension and more detailed treatment of these existing principles, notably: the criteria against which protection adequacy are considered; so-called “Binding Corporate Rules”; and, so-called Commission-approved “Model Clauses”.

What are the next steps?

The European Parliament’s proposed amendments will now be considered by the (EU) Council of Ministers (consisting of all the EU Member States), which may commence soon. When there is agreement within the Council, the Council and the Parliament will have to agree on the final version (with the European Commission acting as a kind of intermediary) so that the proposed reforms can become law - this final part of the process is not expected to be a smooth one, both among the EU Member States within the Council, and between the Council and the Parliament.

The full application of the new Regulation (and Directive) is not anticipated until 2016.

Final words

The above-mentioned elements of the reforms raise many issues, along with other aspects that have not been addressed here. Although the reforms bring some clarity, for example as regards data transfers to third countries, implementing and complying with these particular principles will still present challenges to businesses. Whatever the final political agreement is, the EU data protection reforms will entail a high level of compliance obligations, with significant financial, resource and administrative costs for businesses, that businesses should start factoring into their planning now. A more detailed consideration of certain compliance issues will be the subject of a later article on this website.

André Bywater is a commercial lawyer with Cordery in London where he focuses on regulatory compliance, processes and investigations.

André Bywater, Cordery, Lexis House, 30 Farringdon Street, London EC4A 4HH
Office: +44 (0)207 075 1785
andre.bywater@corderycompliance.com