SUMMER UPDATE - Client Alert: EU Data Protection Regulation FAQs

July 1, 2015

What is this all about?

The EU is in the process of reforming its existing data protection rules. These reforms have been moving slowly through the EU legislative pipeline but in mid-June 2015 these reforms received a boost on the road to becoming adopted. Even though the expected implementation date of these rules is still some way off Cordery strongly recommends that businesses keep an eye firmly on the ball as the reforms go well beyond an upgrade - good planning ahead will pay off to meet the eventual major compliance impact.

What is EU data protection?

The right to privacy is mainly regulated in the EU under a 1995 Directive that controls the processing of personal data. These rules are of very wide effect with major compliance requirements placed on businesses inside and outside the EU.

Why is this change happening?

Three and a half years ago the European Commission officially began the legislative reform process with the overall objective of significantly overhauling the 1995 rules, the mantra being to catch up with the huge advances of the digital age. Other aims include a less administratively burdensome and costly regime for businesses, an extension and expansion of rights, and, making privacy by design the norm.

Are these completely new rules?

Yes and no. Yes, the 1995 rules are being completely replaced. No, not only will the fundamental aspects of privacy continue to be protected, they will also be extended. The reforms essentially build on the current structure, but, the 1995 rules will at least triple in length - or even more depending

on the number of amendments that are eventually accepted under the EU legislative process - the current Council text (see below) consists of some 120 recitals and 80 articles in over 200 pages!

What new rules will there be?

There are in fact two proposed sets of new rules as follows.

Firstly, there is a Regulation, which sets out a general EU framework for data protection, i.e. to replace the 1995 Directive. A Regulation has been chosen because this format should be immediately applicable law once adopted, i.e. it will not require EU Member States to pass further legislation. This said, the latest version proposed by the Council (see below) allows for plenty of carve-outs for the EU Member States. Further, Member States like the UK will still face legislative issues about what to do with aspects of their national data protection rules that are additional to the EU rules.

Secondly, there is a Directive, which specifically deals with protecting personal data processed in a law enforcement context. Most businesses do not need to be too concerned about the Directive but it forms part of a package with the Regulation, and because the Directive has been subject to procedural delay this will likely impact the timing and adoption of the Regulation.

Where do things currently stand?

In very simple terms, three EU institutions are involved in this legislative process: the European Commission ("the Commission"), which acts as the executive body of the EU, proposes the legislation which is jointly adopted by the Council of the European Union ("the Council"), which represents the executive governments of the 28 EU Member States, and, the European Parliament, which is the directly elected parliamentary institution of the EU.

After the Commission began the process the proposal went to the European Parliament who, after over two years of much debate and lobbying, put forward a huge number of amendments. Then it was the turn of the Council who after over a year of consideration recently agreed a "general

approach" (their proposed amended version can be found here - http://bit.ly/1FOet4w) although it is understood that many divergent views within the Council remain.

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

A key aspect of the reforms is that a business which is in several EU Member States should only have to deal with one data protection regulator (called a "supervisory authority" in the Regulation) - most likely this will be in the country where the business is based. Individuals will also only have to deal with their "home" regulator, in their own language, even if their personal data is processed outside their "home" country. But, this one stop shop system is likely to have caveats, for example, under the current Council text, where there is a cross-border data protection issue (such as within the context of a complaint) businesses may have to deal with several data protection regulators. The current Council text also beefs up the tasks and powers of the regulators along with the cooperation mechanism between them. The to-be-created European Data Protection Board (to replace the current "Article 29 Working Party", an important grouping of data protection regulators) will also have as one of its functions to act as a kind of appeals mechanism concerning some issues between the regulators.

Therefore, the implementation of this system, in whatever form it is eventually agreed, is likely to be less of an actual one stop shop in reality and perhaps represents the greatest compliance challenge out of all the reforms for a business. Businesses will still have to be prepared to answer to more than one regulator.

Will I have to register with a regulator?

No. There will no longer be a requirement for a data controller (the person determining the purposes for and manner in which personal data are processed) to register with a data protection regulator, and consequently the payment of a fee to register will also disappear.

But, whilst one administrative burden goes another one apparently appears as data controllers will have the obligation of implementing appropriate measures to be able to demonstrate that the

processing of personal data is in compliance with the Regulation - data processors (processing means carrying out any operation or set of operations, or obtaining, recording or holding the information or data) will also be subject to certain direct obligations.

Further, the disappearance of registration will pose a challenge for many Member State regulators who will lose an income stream from fees for registrations. How will their budgets be impacted and how will this affect their administrative and enforcement capabilities?

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

Yes. The new 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 they process the personal data of EU residents and offer them goods and services, which the current Council text qualifies as being ”irrespective of whether a payment by the data subject [the person concerned] is required”. This extra-territorial dimension is a very significant change and very controversial. A key issue is that it may prove very difficult, if not impossible, to actually enforce this.

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

Yes. 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 beginning, although it should be noted that the current Council text seems to have put some limit on this. Privacy by design and/or default might sound fine as a policy aspiration but its practical application will not always be so straightforward.

Will consent be required for data processing?

The requirements for consent have been recalibrated. Under the current Council text “unambiguous” consent will have to be given by a person in order for their personal data to be processed - there are still some differences though between the Commission, the Parliament and the Council on the way this is worded. Businesses will not be able to rely on silence or opt-outs and

instead an active process such as box-ticking will have to be put in place - the current Council text states that “silence or inactivity should therefore not constitute consent”.

Are there any new rights?

Yes. A series of new rights are introduced including the right to portability (transmitting personal data from one data controller to another), and, the right to not be subject to profiling (subject to certain exceptions). Perhaps most controversial, mainly due to the highlighting of the issue in last year’s European Court of Justice ruling concerning Google, is the introduction of a legislative right to be forgotten (albeit not an absolute right), i.e. the right to have data erased without undue delay where the data are no longer necessary in relation to the purpose for which they were collected or otherwise processed. Much ink has been spilled on the seriously problematic nature of this right, e.g. the technical, logistical and financial costs involved, the possible hampering of law enforcement/regulatory bodies in their investigations, the ability to hide an unsavoury past, and, the impact on free speech. There’s more on the original Google right to be forgotten case here - www.corderycompliance.com/european-court-google-ruling/.

There will also be a more expanded right for people to be provided with information about how their data is used. Further, it should also be noted that under the reforms so-called “subject access requests”, a process whereby someone can exercise their right to gain access to data held on them, must be answered within one month of receipt of the request but which (under the current Council text) may be extended to two months where necessary.

Will I need to appoint a data protection officer?

Possibly. A special data protection officer may have to be appointed to deal with data protection compliance - there are differences between the proposals of the Commission, the Parliament and the Council with the latter being more flexible as they suggest making the appointment of data protection officers discretionary unless made mandatory by either EU or EU Member State law. This may prove to be a flashpoint between the EU institutions in the trilogue process (see below).

When will I have to report data breaches?

There are two reporting obligations. Significant changes concerning the mandatory reporting of data breaches are to be introduced. Data breaches will have to be reported to data protection regulators in each country affected without delay and, where possible, not later than a period to be set under the new rules, which in the current Council text is currently set at 72 hours, but in the final version this may yet change due to differences on this between the Council, the Parliament and the Commission where the other two bodies favour 24 hours. 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.

This does not seem likely to be a one stop shop system, so, for example if you have a breach affecting 12 EU countries you will likely have to make 12 separate reports within the 24 or 72 hours allowed.

Two particular contentious issues that may prove a challenge are:

1. Whether there will be a threshold, i.e. if a breach is minor whether it will have to be notified or not. The current Council text is more business-friendly and suggests a threshold qualifiying a breach as one "which is likely to result in a *high risk* for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to the [sic] reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage"; and,
2. Whether technical measures to secure the data, such as encryption, will mean that a breach need not be reported and if so what those acceptable technical measures will be. This is important for multinationals as US data breach laws commonly provide exceptions for data which is sufficiently encrypted.

These various issues are likely to be a flashpoint between the EU institutions in the trilogue process (see below).

What about liability and compensation?

Under the reforms, both liability and compensation have been beefed up with the current Council text providing that any person who has suffered "material or immaterial damage" due to non-compliant data processing has a right to compensation from "the controller or the processor" for damage suffered.

Because of the extra risk that a data breach may now entail under this new formulation, if eventually adopted, businesses will need to do the maximum to minimise the potential for damages claims.

Will there be mandatory audits?

Probably. Under the new rules regulators may be given the power to carry out surprise audits on businesses. This may prove to be a significant new tool in the regulator's armoury. Businesses are therefore recommended to put in place procedures and train staff to deal with this.

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

Under the new rules, data protection regulators will have the power to impose high fines for infringing the data rules. Three different bands of fines to be applied in relation to three different sets of categories of infringements are envisaged. In the original Commission proposal and under the current Council text this is up to Euro 1 million or up to 2% of the global annual turnover of a business, whichever is the greater, in the highest category of the three bands and infringements, for example those concerning consent, profiling and breach notifications. Under the current Council text, the to-be-created European Data Protection Board will draw up guidelines for fines for the supervisory authorities. It also seems that a procedure on the lines of EU competition/anti-trust enforcement is being envisaged as the process for imposing fines including as regards aggravating and mitigating factors.

The subject of fines is also expected to be a flashpoint in the trilogue process (see below), perhaps a major one, notably because the Parliament in particular is seeking higher figures.

Will some kind of other assessments have to be made?

Where processing operations present specific risks, an assessment of the impact of the envisaged processing operations on the protection of personal data will have to be carried out. There are major differences between the Council and the Parliament on the applicable risk situation, but whatever the final outcome, an assessment will have to address the envisaged processing and evaluate the risks and the measures that would address them.

The current Council text qualifies a "type of processing" for privacy impact assessment as one which in particular uses new technologies and "which is likely to result in a *high risk* for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the [sic] reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage".

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 (including the US) will remain in place, including the requirement that those data flows can only occur where an adequate level of protection is assured by these third countries. The European Data Protection Board may also play a role in this process by advising the Commission.

What the reforms mainly introduce is an extension and more detailed treatment of these existing principles, including the criteria against which protection adequacy are considered (with relevance for the "Safe Harbor" regime), and, so-called "Binding Corporate Rules", the latter which are treated extensively and which the current Council text expands on.

Further, the current Council text also introduces some new safeguards, notably in the form of a legally binding and enforceable instrument between public authorities or bodies, and, an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country, and, an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country.

Whatever the final outcome, businesses' existing arrangements will have to be checked against these.

What are the next steps?

Now that 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. They will be doing this in a process officially called the "trilogue" and monthly meetings for this process until the end of the year have been scheduled (except August) with each meeting to focus on specific aspects of the proposed reforms. This process is not expected to be a smooth, both among the EU Member States within the Council, and between the Council and the Parliament - there will be much horse-trading. Some even speculate that there will be no final deal whilst others say that there is too much at stake for the EU to not adopt new data protection rules.

In addition, the incoming Luxembourg Presidency of the EU (to take over from the current Latvian Presidency) is aiming to agree on a general approach to the law enforcement data protection Directive in the autumn of 2015 to then immediately start its own trilogue procedure in parallel with the proposed Regulation trilogue.

The full application of the new Regulation (and Directive) is not anticipated until 2017 or even 2018.

It should also be noted that it is envisaged that once the Regulation has been adopted the so-called EU Cookies Directive (2002/58) should be *reviewed* in order to clarify the relationship between the two sets of legislation.

In this alert we have done our best to guess at where these negotiations will end up but this is a work in progress still - do check our website at http://www.corderycompliance.com/category/data-protection-privacy/ where we post regular updates.

What should I do now?

Assuming that the new rules are finally adopted, they will bring a high level of compliance obligations, with significant financial, resource (including IT) and administrative costs. Although finalization of the reforms may seem to be some time ahead, the following are ten compliance issues to start considering:

1. Thoroughly review vendor contracts - you will need your vendors' help especially in reporting security breaches very quickly. Make sure that you have the contractual rights to insist on this and make sure that you can hold your vendors to account;
2. Prepare to update everything and prepare new detailed documentation and records ready for production for regulatory inspection - factor this into overhead costs;
3. Review all key practical aspects such as data retention, destruction etc. through all means of collecting data used by the business;
4. Ensure that new aspects such as explicit consent, the right to be forgotten and erasure, and, the right to not be subject to profiling are all included in policies and procedures;
5. Put in place a data breach notification procedure, including detection and response capabilities - consider purchasing special insurance;
6. If applicable, appoint a data protection officer;
7. If applicable, put in place an impact assessment and/or risk analysis policy;
8. Create compliance statements for annual business reports;
9. Train staff on all of the above; and,
10. Set up and undertake regular compliance audits in order to identify and rectify issues.

Cordery offer a fixed fee registration and renewal service for ICO notifications which can include an annual audit. Details are here: www.corderycompliance.com/solutions/privacy-registration-and-renewal/

Details of Cordery's data protection and privacy practice are here: www.corderycompliance.com/data-protection-privacy/ and details of our training solutions are here: www.corderycompliance.com/solutions/training.

For more information please contact Jonathan Armstrong, Gayle McFarlane or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HH
Office: +44 (0)207 075 1784
jonathan.armstrong@corderycompliance.com

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

Gayle McFarlane
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HH
Office: +44 (0)207 075 1786
gayle.mcfarlane@corderycompliance.com