Linklaters

January 2012

Technology Media and Telecommunications.

Data Protection

EU – Data protection reform: Overview

Viviane Reding set out her aims for the reform of the European data protection laws in a speech in Munich on 22 January 2012. She said:

> "*The new rules will help business in three ways. Firstly they create legal certainty. Secondly, they simplify the regulatory environment. And thirdly, they provide clear rules for international transfers*"

This speech was closely followed by the publication of the Commission's official proposals on 25 January 2012. As predicted, it is in the form of a Regulation for general data processing and a Directive for the processing of personal data in police and judicial matters. The rest of this note just considers the Regulation.

Fundamental structure remains

The overall shape of the draft Regulation is much the same as the current Directive. Most of the key concepts have been retained, including a set of largely unchanged general principles[1] and specific processing conditions to process personal data[2].

The Commission has not used this review as an opportunity to make more fundamental changes, such as removing the distinction between data controllers and data processors, differentiating between structured and unstructured electronic data or abolishing the restrictions on transborder dataflow.

Significant impact for businesses

Whilst the Commission has rejected more radical reform, it has made a number of changes to clarify and enhance the current framework. Some of these changes are significant and far-reaching. Have they achieved certainty, simplification and clarity?

[1] Article 5
[2] Article 7 and 9

Contents

Rather than trying to answer this question in one go, we have instead grouped the changes into a number of separate sections set out below:

> *Certainty and the single market* – The use of Regulation will mean a single data protection law applies across the whole of the European Union, though it is likely there will be differences in the way it is interpreted and enforced in practice. In addition, controllers and processors will only have to deal with one regulator, even if they operate across multiple Member States. This is welcome and should also be extended to groups of companies. More details here.

> *Simplification and accountability* – The proposals abolish the general notification obligation and replace it with obligations to be "accountable". This includes mandatory appointment of data protection officers and privacy impact assessments. We consider if this is a genuine simplification of the current rules and a reduction in "red tape". More details here.

> *International transfers and extra-territorial effect* – The new Regulation leaves the current restrictions on transborder dataflow largely in place, though the use of Model Contracts and binding corporate rules will be eased. There are also extra-territorial provisions, which will apply to overseas companies offering goods or services or monitoring individuals in the European Union. More details here.

> *Consent and individual rights* – The rules around consent will be tightened so it will have to be explicit and can be withdrawn at any time. There are also a new right of data portability and a right to be forgotten, though it is not particularly clear how they will operate in practice. More details here.

> *Data security and breach notification* – All data breaches, no matter how minor, will have to be reported to regulators without delay and, where feasible, within 24 hours. These obligations will be difficult to comply with in practice. There are also additional requirements for contracts with data processors. More details here.

> *Sanctions* – The maximum fine for breach of the Regulation will be Euro 1 million or 2% of annual worldwide turnover. For some of the very largest companies this could result in fines in excess of Euro 1 billion. Without further threshold requirements for fines, such as only allowing fines where the breach causes harm to individuals, this could have a chilling effect on business. More details here.

Conclusions

While some of the changes are welcome, there is much for European and international business to be concerned about. The proposals would impose burdensome new obligations on businesses without fully exploiting the potential single market benefits nor the opportunities to simplify the current regime.

The Commission's proposals will now be considered by the Council and the Parliament. The legislation process should take at least a year and then there will be a further two years[3] before the Regulation comes into force. These changes are therefore unlikely to take effect until 2014 at the earliest.

The proposals are available here.

[3] Article 91

Certainty and the single market

"*there will be a regulatory 'one-stop-shop' for businesses for all data protection matters*"

Viviane Reding, Munich, 22 January 2012

One aim of the Commission's proposed reforms is to provide additional certainty to businesses and to help to create a single, consistent data protection framework across the whole of the European Union.

Use of a Regulation

To achieve this aim the Commission has decided to use a Regulation. This will be directly effective in all Member States two years after it is passed, without the need for national implementing legislation.

This will provide significant single market benefits for businesses as the whole of the European Union will have the same data protection law. For example, we produce a report called Data Protected which, amongst other things, reviews the differences in the implementation of the currrent Directive across the European Union (here). If a Regulation is used, most of the European analysis could be removed, but not all of it. Variations between Member State's laws are likely to remain.

Limits on harmonisation

Firstly, some sections of the Regulation allow Member States to pass additional measures on matters such as employment, health and professional secrecy[4]. Some other areas of the Regulation require national transposition, such as the requirement to lay down "effective, proportionate and dissuasive" penalties for breach of these laws[5]. These will inevitably vary from state to state.

Variations over the interpretation of the Regulation are also likely to arise. It relies on principle-based regulation to cater for the wide range of processing and the likelihood of rapid technological change. This principle-based approach is flexible, adaptable and hard to circumvent but also inherently uncertain. The interpretation of difficult concepts, such as the so-called legitimate interest test, depends in part on subjective value judgements reflecting the particular Member State's culture and traditions. Whilst the new Regulation will ensure the approach will be the same across the European Union, the answers will not be.

Finally, differences in the resources and attitudes of national regulators are likely to result in wide variations in enforcement. As our Data Protected report demonstrates, there is a wide discrepancy between the theoretical powers open to national regulatory authorities and the application of those powers in practice.

[4] Articles 80-85
[5] Article 78

A "one-stop-shop" for businesses

This conclusion makes the next question more important: will there be a genuine country of origin rule for European businesses? The draft Regulation states that a "controller" or "processor" established in more than one Member State will only be regulated by the Member State in which it has its main establishment[6].

This change is very welcome. However, it appears that this rule only applies to businesses and not groups of companies. Thus a French company with a branch in Spain need only consider French data protection laws but a French company with a Spanish subsidiary must consider both. An extension of this concept to groups of companies would be hugely beneficial, allowing them to standardise their data protection policies and practices across the single market without the need for local law advice or the need to liaise with multiple national regulators.

[6] Article 51

Simplification and accountability

"*savings [to businesses] will be achieved by a series of measures… by simplifying the regulatory environment and drastically cutting red tape*"

Viviane Reding, Munich, 22 January 2012

The Commission's aim to help business by providing a single market for data protection are supplemented by a desire to simplify the regulatory environment. The proposal's delivery on this aim is somewhat mixed.

Notification obligations abolished

The obligation on controllers to make a general notification about their processing to their national regulator will be abolished. This change is very welcome and the Commission estimates that it will result in savings of approximately Euro 130 million.

However, organisations with more than 250 employees are still obliged to prepare documents detailing all of their processing[7]. This is similar to the information required for a notification and must be provided to regulators on request. Thus the formalities are removed but much of the substance of this obligation remains.

Accountability replaces notification

In place of the general notification obligations, the Commission is proposing a range of additional measures intended to make organisations more accountable.

This includes an obligation on controllers to appoint a data protection officer if: (a) they have more than 250 employees; or (b) their main activity involves systematic monitoring of individuals[8]. The data protection officer will be appointed for a period of at least two years, during which they will have substantial protection from dismissal.

Other obligations include:

> policies and measures – controllers must adopt suitable policies and measure to enable them to demonstrate compliance with the new Regulation[9];

> data protection impact assessments – these must be carried out where processing presents specific risks to data subjects[10]; and

> privacy by design and default – appropriate measures and procedures must be implemented to protect privacy, for example by putting in place access controls preventing access to personal data and ensuring it is deleted when not required[11].

[7] Article 28
[8] Article 35
[9] Article 22(1)
[10] Article 33
[11] Article 23

While these obligations are generally targeted at areas of risk and are not inherently objectionable, they will not reduce "red tape" for many organisations.

Detail in the hands of the Commission

The draft Regulation provides the framework for the new law but the Commission will be given significant control over its application in practice[12]. The Commission will have power to issue delegated legislation over a wide range of matters, for example to:

> clarify the situations in which the legitimate interests test would be satisfied[13];

> expand the information that must be provided to data subjects[14]; and

> determine the situations in which a subject access request will be deemed to be manifestly excessive[15].

These powers could be exercised in a way that makes the draft Regulation extremely burdensome. It is hard to make a proper assessment of this law without a better understanding of the Commission's intentions in this regard.

General simplification

From a more general perspective, it is hard to see this as a "simplification" of the current rules. The draft Regulation contains detailed rules to flesh out the general principles upon which the new framework is based. It has 139 recitals and runs to 91 articles.

The sheer size of the Regulation will make it difficult for many business to get to grips with it. Large businesses will, no doubt, be able to pay for specialist advice or rely on their data protection officer. Others may struggle. At a time when the European Union needs to be more innovative and become more competitive, the Commission should do more to reduce regulatory burdens and go further to protect small and medium-sized enterprises from excessive regulation.

[12] Article 86
[13] Article 6(5)
[14] Article 14(7)
[15] Article 12(5)

International transfers and extra-territorial effect

"*in a world where the free flow of data is fundamental to business models and physical boundaries are meaningless, we need to rethink the way we transfer data*"

Viviane Reding, Munich, 22 January 2012

The problems with the current rules on transborder dataflow are well recognised. Unfortunately, the current framework has been largely retained with only minor improvements to the use of Model Clauses and binding corporate rules. The proposals also contain extra-territorial provisions extending the Regulation's reach to some companies based outside the European Union.

Restrictions on transborder dataflow largely untouched

The new Regulation does not do anything radical to the current framework for transfers of personal data outside of the EEA, such as replacing it with a more general accountability obligation. Any transfer to a jurisdiction outside of the EEA must still be:

> to a "whitelisted" jurisdiction providing adequate protection. Adequacy findings under the current Directive will still count under the new Regulation[16];

> made on the basis of a "structural" compliance mechanism, such as binding corporate rules or Model Clauses (see below)[17]; or

> in reliance on a derogation, such as consent from the relevant data subject to the transfer[18].

There is one important new derogation[19]. This allows the transfer of personal data to a country outside of the EEA if: (a) the transfer is not "frequent or massive"; (b) appropriate safeguards are in place; and (c) details of the transfer are documented and the national regulatory authority is informed.

This derogation replaces some of the opaque justifications for transborder dataflow under the current Directive. By way of example, the UK implementation allowed data controllers to make transfers based on their own self-assessment of the level of protection once the transfer takes place. This would not be possible under the new framework and the much more restrictive terms of the new derogation would apply instead.

Boost for binding corporate rules and Model Clauses

The new Regulation eases the use of Model Clause by abolishing any obligation to have them notified to, or approved by, a national regulator[20]. This should make them significantly easier to use in practice.

[16] Article 41
[17] Article 42
[18] Article 44
[19] Article 44(1)(h)
[20] Article 42(3)

It also codifies many of the soft-law rules on binding corporate rules developed by the Article 29 Working Party[21]. The substance of these binding corporate rules will be much the same and they must still be legally binding and provide enforceable rights to individuals. However, the approvals process has been simplified so that an application will only need to be made to one data protection authority, which will then consider it in conjunction with the other authorities through a so-called consistency mechanism. Once approved by the data protection authority, no further authorisations or filings will be required.

The regulation makes it clear that groups of processors can also use binding corporate rules, which should make outsourcing and cloud computing much easier.

Extra-territorial application

The new Regulations also contains new, and controversial, extra-territorial provisions. Organisations processing personal data about European residents will be subject to the Regulation if they:

> offer goods or services to data subjects in the European Union; or

> monitor behaviour of those data subjects[22].

It will be interesting to see how these rules are enforced in practice. The focus is likely to be on the big US tech companies. Some of these companies have deliberately kept much of their data processing in the US in the past to avoid becoming subject to the current Directive. They will now find it more difficult to avoid the net and many may be a tempted to establish themselves in a friendly jurisdiction within the European Union, such as Ireland, and utilise the single market provisions in the Regulation to avoid some of the more enthusiastic national regulators.

For other foreign data controllers, the position is less clear. It will be interesting to see how much appetite the data protection regulators have to pursue these entities, given the practical difficulties of enforcing sanctions against them in practice.

[21] Article 43
[22] Article 3(2)

Consent and rights for individuals

"*the reform will give individuals better control over their own data*"

Viviane Reding, Munich, 22 January 2012

The new rules are intended to provide individuals with much better control over their personal data with provisions specifically targeting new forms of media such as social networking sites.

Consent

The rules around consent have been tightened considerably[23]. In particular:

> consent must be "explicit" and result from an affirmative action or statement. This is in addition to the existing requirements that it be "freely given, specific and informed". This will, rather obviously, prevent controllers arguing that the data subject has given implied consent;

> consent can be withdrawn at any time. There was some uncertainty if this was the case under the old Directive;

> written consent must be separate from any other relevant matter. This suggests that it will not, for example, be possible to gain an individual's consent as result of them just agreeing to a general set of terms and conditions; and

> consent will not apply where there is a "significant imbalance between the position of the data subject and the controller". This may make it difficult to rely on consent in the employment context (as is currently the case) but it is unclear how it would apply in other cases. For example, is there always an imbalance between consumers and the companies that they deal with?

The collection and use of children's information online will require consent from the child's parent or guardian. For these purposes a child is someone under 13 years old.

"Right to be forgotten"

This is one of the most high-profile changes under the new Regulations, giving individuals the right to erase embarrassing misdemeanours from Facebook and the like[24]. The provisions are, however, of general application and not limited to the online world.

The right itself is somewhat confusing and seems to largely repeat other provisions of the Regulation such as the right to withdraw consent, the right to object to processing and the obligation to delete data when there is no longer a legal ground to do so. The right is also heavily caveated where the processing is in the public interest or erasure would compromise freedom of expression.

[23] Article 4(8) and 7
[24] Article 17

This new right may have received a considerable amount of interest but it is still unclear how it would operate in practice.

Data portability

In keeping with the general interest in cloud computing, there are also specific rules on data portability[25]. Individuals will have the right to receive copies of their personal data in electronic form so long it is stored in a structured and commonly used format. The individual must also have the right to provide that data to another provider.

[25] Article 18

Data security and breach notification

"*Companies that suffer a data leak must inform the data protection authorities and the individuals concerned, and they must do without undue delay. As a general rule, without undue delay means for me within 24 hours*"

Viviane Reding, Munich, 22 January 2012

The draft Regulation contains both enhanced security obligations and new notice of breach laws. The notice of breach laws mirror the problematic provisions in the amended ePrivacy Directive. They will be extremely difficult to comply with and, in many cases, serve no useful purpose.

Breach notification

The trigger for the notification is a "personal data breach" being any breach of security leading to disclosure, destruction, loss or destruction of personal data[26]. There are a number of points to note:

> there is no *de minimis* exception. The notification obligation will be triggered even if: (a) only one person's information is involved; or (b) all of the information is public; and

> there is no exception if the data is protected. Even if the information is subject to very strong encryption, such that it could never reasonably be accessed, it is still necessary to make a notification.

All "personal data breaches" must be notified to the relevant data protection authority without undue delay and where feasible within 24 hours of the controller becoming aware of it. The notification must provide a range of details including details of the data lost, a description of the consequences of the breach and steps taken to mitigate those consequences. Again, there are a number of points to note:

> the time requirement does not revolve around business hours. Presumably data controllers will need an out-of-hours response team to make these notification where, for example, an employee loses his Blackberry on a Friday night;

> it's not clear how the awareness qualification works. Is the controller "aware" of the breach as soon as one of its employees becomes aware or only when it is reported through the appropriate channels; and

> in many cases it will be impossible to obtain sufficient information within the 24 hour deadline[27]. As such many reports will be incomplete.

Data subjects must also be notified of the personal data breach without undue delay unless the relevant information was protected or the personal data breach would not adversely affect them.

[26] Article 4(9) and 31

[27] The 24 hours deadline does not apply if it is not feasible to meet it and the notification is accompanied by a justification for the delay. In practice, many data controllers may try and compromise on the detail in the notification to try and meet the strict deadline.

Data security obligations

The main amendment to the remaining data security provisions affects the engagement of processors[28]. Controllers would have to impose a number of additional obligations on their processors including:

> preventing the processor from using sub-processors without their consent;

> ensuring it returns all personal data at the end of the contract; and

> obliging it to co-operate with any investigation by a relevant data protection authority.

Use by a processor outside the scope of its instructions will mean it becomes a controller. Finally, processors will become directly liable for compliance with many provisions of the Regulation.

[28] Article 30

Sanctions

"*all data protection authorities … will have the same adequate tools and powers to enforce … this will give the legislation the necessary 'teeth' so rules can be enforced*"

Viviane Reding, Munich, 22 January 2012

The proposed reforms will bring about a significant increase in the sanctions for breach of data protection laws. The potential size of these fines and the residual uncertainties in the Regulations framework risks a chilling effect on business.

Fines of up to 2% of global turnover

The new Regulation sets out a tiered regime[29]. The national regulator can impose:

> fines of up to Euro 250,000 or 0.5% of annual worldwide turnover for less serious breaches, such as improperly charging a fee to respond to subject access requests;

> fines of up to Euro 500,000 or 1% of annual worldwide turnover for medium-level breaches. This includes having an inadequate privacy policy, failure to comply with the right to be forgotten and failing to keep a record of the types of processing undertaken; and

> fines of up to Euro 1,000,000 or 2% of annual worldwide turnover for serious breaches. This covers the largest category of potential breaches including processing data without satisfying a processing condition, not designating a data protection officer or failing to notify a regulator of a security breach.

The fines are significant. For some of the very largest companies fines could, theoretically, exceed Euro 1 billion.

National regulators will also have other powers, such as the right to order the erasure of data[30] and Member States must ensure that these fining powers are supplemented by range of other effective, proportionate and dissuasive penalties[31], for example criminal sanctions.

A chilling effect?

National regulators are obliged to consider a range of factors before determining the level of the fine, including the gravity of the breach and the *mens rea* of the data controller. Whilst it is hoped this will ensure that fines are applied in a sensible manner, there is a risk that they may be completely unjustified by the breach in question.

[29] Article 79
[30] Article 53
[31] Article 78

This could have a chilling effect on decision-making by businesses. For example, the highest tier of fines applies to a wide range of breaches including failing to satisfy a processing condition. This question of whether a processing condition is satisfied is controversial and one on which there are significant differences of opinion not only amongst data protection lawyers but also among regulators and the courts (particularly in the case of the so-called legitimate interests test). Businesses are much more likely to act conservatively under the threat of significant fines for getting this assessment wrong. Whilst this may prevent some breaches, it is also likely to prevent many legitimate business activities.

It would be much better if fines were dependent on the gravity of the breach so that, for example, a precondition for any fine[32] is that there is a clear breach that causes serious harm to data subjects and was committed intentionally or recklessly.

Contacts

For further information please contact:

Peter Church
Solicitor

(+44) 20 7456 4395

peter.church@linklaters.com

Author: Peter Church

One Silk Street
London EC2Y 8HQ

Telephone (+44) 20 7456 2000
Facsimile (+44) 20 7456 2222

Linklaters.com

[32] Currently there is some protection under Article 79(3) but it is very limited. A national regulatory authority *may* give a warning on a first and non-intentional breach but *only* if the relevant controller has less than 250 employees and its processing is ancillary to its main activities.