Reform of Europe’s data protection regime moved one step closer this January with the publication of the Commission’s long awaited ‘General Data Protection Regulation’ (the ‘Regulation’). The proposal is the culmination of over two years of consultation and review. The new Regulation, which is intended to replace the current Data Protection Directive, was published alongside a new draft Directive covering the police and judicial sector. They will both undergo a period of review and the Commission has indicated it aims to have a final agreed legislative framework in place by 2014. In this briefing we focus on the draft Regulation and the changes it may bring.

**WHY DID THE CURRENT REGIME NEED TO CHANGE?**

The objectives and principles of the current European data protection framework are still regarded by many, including the Commission, as sound. The new Regulation therefore retains many of the current concepts, definitions and basic principles.

However, for a number of years the regime has been criticised for being inconsistent and out of date. For example, the different ways in which Member States implemented and interpreted the Directive had led to a lack of harmonisation. In the UK, the Information Commissioner recognised the need for review, stating in his initial response to the Commission’s proposal that ‘there is no doubt that the EU’s legal framework for data protection needs modernising in the face of increasingly sophisticated information systems, global information networks, mass information sharing, the ever growing online collection of personal data and the increasing feeling of individuals that they have lost control of their personal information. The proposal seeks to address these needs’.

While the Commission’s proposal may seek to address the needs, or problems, with the current system, how successful it has been in doing so is currently under debate.

**WHAT ARE THE KEY CHANGES?**

The instrument itself
The first obvious change is the fact that the new proposal is in the form of a Regulation, rather than a Directive. A Regulation is directly applicable in all Member States, whereas a Directive requires further national legislation to bring it into force in the different jurisdiction.

---

1 Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation).
2 Directive 95/46/EC
3 For example, Page2 of the Explanatory Memorandum of the Regulation
The second is the length. The draft Regulation is much longer than the current Directive – it has 91 Articles compared to the current Directive’s 34. In part this is because it recognises concepts, like Binding Corporate Rules, that have developed since the publication of the current Directive, and introduces new concepts (such as reporting security breaches) which have been under discussion for some time. However, the increased length is also due to the fact that the new regime is a lot more prescriptive than the current Directive. In addition there are many provisions which enable the Commission to prescribe more detail on a particular matter by adopting ‘delegated acts’, and/or laying down standard formats for notifications, communications and the like.  

Increased Harmonisation
The fact that the new law is a Regulation, and that it is more prescriptive than the current regime, will help create a more unified data protection regime across the Member States. The Regulation also contains a consistency mechanism which aims to ensure ‘unity of application’ in relation to processing which affects several member states. Increased harmonisation is a good thing for many multi-national organisations which have struggled with the current lack of uniformity across Europe. However, there are still likely to be differences in the way Member States interpret and enforce the Regulation. The Regulation also allows Member States to pass additional measures for certain matters (for example health and employment) which will lead to further divergences.

Also, increased harmonisation may feel like increased regulation for many UK data controllers, who are used to a more flexible regime, and regulator, than in some other parts of Europe. Both the UK Government and regulator (the Information Commissioner’s Office or ‘ICO’) have expressed concerns about an overly prescriptive regime. Back in May 2011, Justice Secretary Ken Clarke issued a warning that the imposition of a detailed, inflexible data protection regime on the whole of Europe without regard to different cultures and legal systems carried with it serious risks. This February, in its initial response to the draft Regulation, the ICO also criticised the proposals for being ‘unnecessarily and unhelpfully over-prescriptive’ in certain areas, commenting that this risks encouraging a ‘tick-box’ approach to data protection compliance.

The reach of the regime and the regulators
The current rules on when a particular piece of European data protection law applies (and consequently which EU data protection authority has jurisdiction) are complex. At present it depends on where the data controller is established, or where it ‘makes use’ of equipment. The new proposals change this:

• Extra-territorial reach: The regime still applies to those established in the EU. However, it would also apply to data controllers based outside the EU who process the personal data of EU residents when offering them goods or services or monitoring their behaviour. This could apply to US and other non EU on-line businesses who have purposely kept their operations out of the EU to date. However, much of the detail relating to this is currently unclear, for example what exactly constitutes ‘offering’ goods and services to EU residents and how in practice will the EU regulators be able to enforce the regime outside of Europe?

• There will be a ‘one-stop-shop’ (or lead) regulator: Data controllers will only need to deal with a single national data protection authority in the EU country where they have their main establishment. This is helpful for multi-national organisations, although not as useful as it could have been. It seems to stop short of allowing group companies to benefit from the ‘one-stop-shop’ rule. It may also be difficult, as drafted, for organisations with

---

4 For example Articles 31(6) and 32(6)
5 Article 80-85
6 In a speech to the British Chamber of Commerce, May 2011
7 Article 3
8 Article 51(2)
complex structures to determine the location of their ‘main establishment’ and it is not clear how it will work where controllers are not established in the EU. Further clarification is required in relation to this provision.

The provisions
While the broad principles have remained largely the same, the draft Regulation introduces many changes. These range from smaller definition changes, to new concepts, procedures and roles. Some of the key changes are set out below:

Changes to the definitions of data subject, personal data and sensitive personal data
While many of the definitions contained in the current Directive continue to be used in the Regulation, some have been added to, amended or changed. For example the definitions of data subject and personal data have been split and more detail has been added to try to clarify that on-line identifiers such as IP addresses can be used as well as more ‘traditional’ identifiers. This could result in a widening of the definition, particularly for those who operate in the on-line world.

Unfortunately it seems that there may still be some confusion around the definition of personal data. Recital 24 of the draft Regulation creates some confusion as it states that identification numbers, location data and on-line identifiers ‘need not necessarily be considered as personal data in all circumstances.’ Also, in the UK, following the English Court of Appeal’s decision in Durant v FSA,9 there has been some debate over the breadth of the definition of personal data, and in particular what information ‘relates’ to a data subject. This debate looks set to continue as the draft Regulation’s definition of personal data still uses the terminology ‘information “relating to” the data subject’.

The definitions relating to ‘special categories of personal data’ (Sensitive Personal Data under the Data Protection Act 1998) have been retained,10 and added to. For example, new definitions of genetic and biometric data and data concerning health have been added to the list of ‘special categories of personal data’ worthy of additional protection. There has, however, been no extension to cover financial data, which many people would consider to be ‘sensitive’.

There have also been slight changes to the wording relating to religious beliefs. The current Directive states that data revealing ‘religious or philosophical beliefs’ should be protected as ‘special’ or ‘sensitive’ data whilst the draft Regulation refers only to ‘religion or beliefs.’ The ICO has expressed concerns that this new drafting is too wide, citing a case in the UK where it was argued that a belief in climate change was a belief which should be protected.

Consent
The draft Regulation adds a new provision that all consent must be ‘explicit’. Previously this was only required where consent was obtained to process sensitive personal data. The commentary in the draft Regulation states this is added to ‘avoid confusing parallelism with “unambiguous” consent’ and to have ‘one single and consistent definition of consent’.

The draft Regulation sets out further conditions for consent.11 These clarify that implied consent is no longer an option, which may be difficult for some data controllers, particularly those operating in the on-line world. They also require that consent given in a written declaration must be distinguishable from any other matters dealt with in the declaration. This may mean that data controllers who obtain consent via their general terms and conditions will need to re-think how to present the consent requirements within such terms, for example by including a separate tick-box.

---

9 Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746
10 The ICO has previously expressed doubts as to the value of protecting special, or sensitive categories of personal data. See the ICO’s initial analysis of the European Commission’s proposals for a revised data protection legislative framework, 27 February 2012.
11 Article 7
The new rules also clarify that consent will not provide a legal basis for processing where there is a significant imbalance between the position of the data controller and data subject. This is likely to cause more problems in the already difficult area of employee consent and with respect to children. For example, parental consent will be required where a data subject is under 13 years old.

**Legitimate interest**

The legitimate interest condition is heavily relied on in practice by many data controllers. While it remains largely unchanged, there are some amendments which could have practical consequences. The changes include:

- a narrowing of the condition so that it only applies where processing is in the legitimate interests of the data controller. Under the current Directive this also applies to the legitimate interests of ‘third parties to whom the data are disclosed.’ There is no commentary in the Recitals as to why this change has been made, and the European Data Protection Supervisor describes the change as ‘unexplained’ in his commentary on the reform package. However, given the wide reliance placed on this processing condition, the change could be problematic for some data controllers;

- an express reference to the particular care which must be taken when relying on this condition where the data subject is a child. The draft Regulation gives the Commission the power to adopt delegated legislation relating to the legitimate interest condition for various sectors and data processing conditions, including in relation to the processing of children’s personal data;

- an express prohibition on public authorities relying on the legitimate interest condition in the performance of their tasks. The ICO cites this as one reason why the draft Regulation may make it difficult for the public sector to process personal data which is necessary but not specifically provided for in law;

- a change to the right of data subjects to object to processing. Currently where processing is based on the legitimate interest condition data subjects can object to it ‘on compelling legitimate grounds.’ Under the draft Regulation the burden of proof has shifted so the data subject could object unless the controller demonstrates ‘compelling legitimate grounds’ for the processing which override the interests of the data subject.

The Recitals also provide commentary on the legitimate interest condition. For example, they state that to ensure transparency, the data controller should be obliged to ‘explicitly inform the data subject on the legitimate interests pursued and on the right to object’ and to document those interests.

**The scrapping of notification/registration requirements**

Many data controllers will be glad that they no longer need to register with their local data protection authority. The Commission have highlighted this as one of the ways that they are cutting ‘unnecessary administrative requirements’ and saving businesses money (estimating that the notification requirements cost businesses...
around €130 million a year). However, registration/notification has been replaced by a requirement for increased ‘responsibility’ and ‘accountability’ for those processing personal data, which arguably places an equivalent administrative burden on data controllers (see below).

Accountability

The concept of accountability was discussed prior to the draft Regulation being published. For example, there was a working party paper in July 2010 which put forward a proposal for a principle on accountability which would require data controllers to put in place ‘appropriate and effective measures to ensure that the principles and obligations … are complied with and to demonstrate so to supervisory authorities upon request.’ The aim was to help move data protection from ‘theory to practice’ and to help the regulators in their supervisory task.

While the draft Regulation does not contain an article entitled ‘Accountability’, it does contain provisions which ‘take account’ of the accountability debate. These include an obligation to:

- adopt policies and implement measures to ensure compliance with the Regulation and verify those measures (possibly by the use of independent auditors);
- notify data breaches, ideally within 24 hours of the breach. It is not surprising the proposal includes an obligation to notify security breaches. Currently this only applies in law to ISPs and Telcos, although ICO good practice guidance expects all data controllers to notify a breach if certain conditions/thresholds are met. However, it is unfortunate that the current drafting includes unrealistic timeframes and detailed information requirements, and fails to limit the obligation to serious or material breaches. The Commission does have the power to adopt delegated legislation in relation to security breaches, including to further specify the particular circumstances in which a data breach notification is required. However, it is unclear when, or if, this delegated legislation may be passed;
- keep detailed records of all processing, unless there are less than 250 employees and data processing is ancillary to the main activities. Interestingly, the information which must be kept (the purposes of processing, categories of data subjects etc) is similar to that required under the current notification regime. The draft Regulation therefore does not dispatch with the need to collect certain information. Rather it changes the obligation from an external facing obligation to notify with a regulator, to an internal obligation to keep records which may be inspected. Also, as a general point, there seems to be a greater level of information which must be recorded and disseminated under the proposed new regime. For example, more detail must be provided to data subjects when their information is collected (the fair processing information), and some of the categories may be more difficult for data controllers to satisfy (such as the requirement to tell data subjects at the point of collection how long their data will be kept);
- follow ‘data protection by design and default’ principles. These include implementing appropriate technical and organisational measures and procedures, ensuring data is only processed where and for as long as necessary and generally complying with security obligations;

20 Article 22
22 Explanatory Memorandum to the Proposal for a General Data Protection Regulation, paragraph 3.4.4.
23 Article 22(3)
24 Article 31
25 Article 4(3) of the E-Privacy Directive 2002/58/EC
26 Article 28. This is one of a number of exemptions or thresholds which apply to limit the burden on SMEs.
27 Article 23
• carry out a data protection impact assessment prior to 'risky processing operations'. The Regulation sets out both a list of operations which present specific risks and details of what an assessment should contain;

• appoint a data protection officer where the processing is by a public body or enterprise employing 250 persons or more, or where the core activities of the data controller/data processor require 'regular and systematic monitoring of data subjects'. This obligation builds on a provision in the current Directive which allows Member States to exempt data controllers from the notification requirements where they appoint a 'data protection official'. While it will be a new provision for UK data controllers, it is a post currently provided for in some other Member States such as France and Germany.

The accountability principles can also be found in the main data protection principles themselves. They clarify that personal data must be processed under the responsibility and liability of the controller who shall ensure and demonstrate compliance with the Regulation for each processing operation.

Direct obligations for data processors
The current regime focuses obligations on the data controller rather than data processor. While the draft Regulation keeps the concepts of data controller and data processor, it imposes obligations directly on data processors. These include an obligation to keep documentation of all processing under its responsibility, to appoint a data protection officer if certain thresholds are met and to be liable for certain fines where there has been a breach. It also requires that more detail is included in the data processing contract. For example, the contract must stipulate that the controller’s prior permission is required if the processor wishes to sub-contract and that a data processor which processes personal data outside of its instructions will be considered a joint data controller and subject to the rules on joint data controllers laid down in the draft Regulation. These changes will make the relationship between data controllers and those traditionally classified as data processors much more complex. They take away much of the current incentive for service providers to classify themselves as processors, and may lead to service providers pushing for a more even allocation of risk in the processor contracts.

International Transfers
The general prohibition on transferring personal data outside the EEA without adequate protection remains, as do many of the ways in which adequate protection can be achieved. There have been some changes. For example, the draft Regulation legally recognises the concept of Binding Corporate Rules. It simplifies the approval process and extends the concept to processors and ‘a group of undertakings’. The draft Regulation also introduces a new derogation, allowing transfers which are necessary for the controller’s (or processor’s) legitimate interest, provided a number of conditions have been met. These include ensuring the transfers are not ‘frequent or massive’ (although these terms are not defined) and informing the regulator of the transfer. However, there has been no ‘radical re-think’ on international transfers, which is something the ICO had previously called for. In fact, the draft Regulation takes away some of the flexibility the ICO had built into the UK system, such as an ability for data controllers to make their own adequacy assessment when transferring data. It also requires more involvement from the Regulator. For example it requires approval by the data protection authority of certain contractual clauses.
of the key criticisms of the current regime is its failure to meet the needs of today’s global business environment. It is therefore disappointing that the draft Regulation missed an opportunity to radically re-assess the rules on international transfers.

**New rights for data subjects**

These include a new right to be forgotten and a right to data portability:

- The right to be forgotten has received a lot of press coverage. In part this is due to concerns about whether it would work in practice and whether it could impinge on freedom of expression. The Commission’s aim is to help people ‘better manage data protection risks online’. It involves a right to obtain from the data controller the erasure of personal data where, for example, the data subject withdraws consent. That data controller would then be responsible for taking all reasonable steps to inform third parties who are processing the personal data that a request for erasure has been made (where the controller is responsible for/has authorised the publication).

- The data portability provisions aim to help people transfer their personal data from one service provider to another more easily and improve competition. They give a data subject the right to transfer data from one electronic system to another and to obtain a copy of data where it is processed electronically and in a commonly used format. It may help those who use cloud and similar IT services and who want to avoid being locked in to one service provider. However, again there is uncertainty about how the right would work in practice. For example, given that there is no obligation for data to be processed in a commonly used format, one concern is that data controllers will try to circumvent the rules by avoiding the use of standard/commonly used formats.

**Increased sanctions and fines**

There are many ways in which the current regime seeks to raise the profile of, and confidence in, data protection. They range from encouraging incentives for compliance, such as certification mechanisms and Data Protection seals and marks, to having new sanctions and powers. The latter include new investigatory powers and ‘competition style’ fines.

The fines have received the most press coverage. Although they are not quite as big as originally feared (an unofficial draft of the Regulation leaked in 2011 included fines of up to 5% annual worldwide turnover) they are still very large. They range from ‘up to’ €250,000 to ‘up to’ €1,000,000. Where an enterprise is involved, they range from ‘up to’ 0.5% to ‘up to’ 2% of an ‘enterprise’s’ annual worldwide turnover.

There are some conditions which must be considered when the level of a fine is fixed, such as the gravity and duration of the breach. However, the list of breaches which can trigger the highest fine is long, and could relate to procedural or record keeping failures. The ICO recognises that the fines as drafted fail to link an administrative failure to a risk to privacy. They also recognise that whilst the ‘up to’ wording could result in modest fines, they; ‘take the maxima in the Regulation as being more indicative of the level of fine that could and perhaps would be expected to be imposed’ in which case the categories of breaches listed require further thought. If the intention

---

36 Article 17
37 Article 18
38 Article 39
39 Article 53
40 Article 79
41 See the ICO’s initial analysis of the European Commission’s proposals for a revised data protection legislative framework, 27 February 2012.
of the new regime is to make data protection compliance part of the genetic make-up of European organisations, it may explain why procedural failures (such as failure to carry out a privacy impact assessment) can result in fines. Whether the fines will be reduced or changed as part of the negotiation process remains to be seen. However, by catching the attention of both the media and business community, they have arguably already helped raise the profile of data protection compliance.

COMMENT

The Commission is heralding the new regime as a comprehensive reform which will increase users’ control of their data and cut costs for businesses – in its press release the Commission suggests it will lead to savings of around €2.3 billion.

‘Comprehensive reform’ has not led to a complete overhaul of the current system. Despite calls for some radical re-thinking around certain areas, for example sensitive personal data and international transfers, many of the current proposals build upon existing provisions or acknowledged best practice.

That said, there are new provisions and concepts. For example, the principles around accountability (privacy impact assessments etc.) should help encourage businesses to build data protection compliance into the fabric of their organisation. And the high levels of fines currently under discussion, although worrying for organisations, should raise the profile of compliance to board level.

The new attempts at increased harmonisation should also help multi-nationals streamline their European compliance programmes. However, for many UK based businesses, even those which are part of larger organisations, it is difficult to see where major cost savings will come from. Even where red-tape has been reduced (for example the scrapping of the notification requirement) additional obligations mean that a similar, or higher, level of resources will be required to meet the new obligations.

Also, the length of the draft Regulation and level of detail involved mean that many data controllers may struggle to fully understand what the new regime will mean to them. The ability of the Commission to add further detail to the proposals means that even those that do understand this draft are not yet able to fully assess the impact of this new regime.

Over the next few years we can expect much debate and commentary on the draft Regulation which may help clarify some of this uncertainty. Indeed many interested parties have already published their initial response to the proposals. While Europe as a whole will be watching developments, in the UK, it will be particularly interesting to see how the Government reacts, given its pledge to reduce red-tape for British Business.

This briefing was written by Rob Sumroy, head of Slaughter and May’s Technology and Outsourcing practices, and Natalie Donovan, the Technology and Outsourcing professional support lawyer. If you would like more information on any of the issues raised in this briefing, or would like to discuss technology, outsourcing or data protection matters generally, please contact Rob Sumroy or your usual Slaughter and May contact.

See for example the ICO’s initial response on 25 January and initial analysis on 27 February 2012, the Opinion of the European Data Protection Supervisor on 7 March 2012 and the Article 29 Working Party’s Opinion (WP 191) on 23 March 2012. In the UK the Ministry of Justice released a ‘Call for Evidence’ on the proposals which ran from 7 February to 6 March 2012.