The EU data protection directive

The European Union has a complex and comprehensive data protection regime, introduced in 1998 through EU Directive 95/46/EC and its national implementing laws in each of the EU member states.

This briefing note provides an introduction to the regime – its very broad scope, its key requirements and restrictions, the extent to which the Directive has created – or failed to create – a harmonised data protection regime across the EU – and an indication of the likely development of the regime over the coming years.

Purpose and approach

The purpose of the Directive is to protect the privacy of individuals with regard to the "processing" of their "personal data" while at the same time avoiding putting barriers in the way of transfers of personal data between the EU member states. It requires each member state to impose a series of requirements and restrictions which apply to the processing of personal data.

It is important to appreciate that the scope of EU data protection laws is extremely broad. Although the Directive is aimed at protecting "privacy", it does not simply regulate what one might ordinarily think of as invasions of personal privacy. Its requirements and restrictions need to be taken into account wherever "personal data" are "processed", even if the processing has no privacy implications, and, as we shall see below, the terms "personal data" and "processed" are both defined extremely broadly.

The general approach of the regime is not to identify and outlaw particular bad practices (covert monitoring of personal communications, for example, or lax IT security) but to impose very general requirements and restrictions which must be taken into account whenever personal data are processed.

The key elements of the regime are:

- broad principles of good data protection practice, which must be met whenever personal data are processed
- some specific rules which apply to particular categories of data (e.g. health data) or particular kinds of processing (e.g. transfer outside the EU)
- formal requirements to make filings with or seek approvals from data protection authorities or to appoint internal data protection officers
- rights which can be accessed by "data subjects" (the individuals to whom personal data relate) – e.g. rights of access to personal data held about them, and to correct inaccurate data.

We will first consider the scope of the regime and how it applies to persons involved in the processing of personal data, then briefly look at each of these key elements in turn.

Whilst this approach may meet with resistance from member state governments and data protection authorities it is likely to be welcomed by business as allowing a consistent approach to data protection issues to be taken across the EU.

In most other respects, however, the proposed Regulation will increase the compliance burden facing organisations which process personal data. The proposal includes many provisions which are likely to be strongly resisted by business, particularly in member states where the Directive has been implemented with a relatively light touch. We understand that the proposal has already proved controversial within the Commission itself; and the UK Information Commissioner's immediate response described the proposal as "unnecessarily and unhelpfully over prescriptive".

In this briefing note we identify some key respects in which the Regulation, if passed in its current form, would increase the regulatory burden facing business. We also draw attention to a few examples of welcome proposed ***reductions*** in the data protection regulatory burden

.

This briefing note will be followed by a similar note on the Commission's new proposed Directive on processing of personal data in relation to the prosecution (etc.) of crime (published simultaneously with the proposed Regulation) and, as the Regulation goes through the legislative process, a series of more detailed notes on some of the key issues raised by the proposal.

Highlights of the proposal

1. **Harmonisation (A21/54)**

   The Commission's decision to propose a Regulation rather than a replacement Directive is likely to be welcomed by those tasked with complying with data protection law across Europe, although it may be resisted by national legislatures and authorities keen to preserve particular features of their local regimes. In general, adoption of a Regulation should ensure consistency of data protection standards across the European Union and the wider European Economic Area.

   Note, however, that the proposed Regulation includes a specific exception allowing member states to make their own rules in relation to the processing of personal data in the employment context (article 82). Some member states have introduced specific rules on the processing of employee data which are extremely burdensome for employers and will presumably be preserved despite the implementation of the Regulation. The proposed Regulation also leaves some scope for interpretation of its principles by national data protection authorities and courts, although ultimately subject to appeal at the European level; and, although it proposes a harmonised data protection standard it is in most respects not clear that it actually prevents any member state from passing separate and complimentary laws which are stricter – a key exception being that, as in the current Directive, restrictions on the free movement of data within the EU are prohibited (article 1(3)). Given the nature of and background to the Regulation it is likely to be regarded as setting a maximum standard where it does not positively allow for the contrary, but this is not certain and would ideally be made clear in future drafts. It remains to be seen, therefore, to what extent the Commission's objective of a truly harmonised regime will be achieved – and of course the negotiation process leading to the Regulation coming into force may introduce further derogations allowing local variation.

   The Regulation (article 21) also allows member states to derogate from its requirements by legislation, where necessary for various "public interest" purposes such as public security and the investigation of crime. The

Key issues

- An (almost) harmonised EU data privacy regime
- Broad definition of "personal data"
- Extended extra-territorial effect
- No solution to the international transfer conundrum
- Notification regime given up
- New requirements for data privacy bureaucracies
- Increased compliance burden in most areas.

Proposal published at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

member states will presumably seek to enshrine the existing derogations, set out in the national laws implementing the Directive, in laws designed to provide exceptions to the Regulation. We would expect the UK, for example, to seek to exploit the permitted derogations to the full. It would be preferable if, in future drafts, minimum exceptions could be spelt out on a harmonised, pan-European basis.

Harmonisation of course also has its disadvantages. From a UK perspective, for example, the harmonisation is for the most part towards a higher level of protection, and legislation by Regulation rather than Directive means that (except where the derogations are available) the UK legislature loses the chance, exploited in the UK implementation of the Directive, to spell out for the UK courts how it interprets the rather general rules drafted at the European level. This issue will arise to one extent or another in all member states.

On a slightly different note, the Regulation gives the Commission discretion in many areas to specify its requirements by subsequent secondary legislation which would be subject to comparatively little scrutiny by the member states. The regime established by the Regulation could be considerably more or less onerous depending on the approach taken by the Commission in these areas. It would be preferable, to the extent possible, to legislate more specifically during the period leading to the Regulation coming into force. In practice, however, the basic provisions of the Regulation are likely to be sufficiently controversial to take up all the available attention during this period.

Note, finally, that the proposal includes a cumbersome "consistency" process (article 57) through which the data protection authorities of all the member states, plus the Commission, will need to be consulted before a wide range of steps are taken on a national level (including, for example, the approval of binding corporate rules), with the possibility that steps may be rejected by vote on a simple majority basis. It remains to be seen how this will work in practice but it suggests an increased power of the majority group within the data protection authorities to dictate how the Regulation is implemented in practice – and their track record, through the article 29 working party established under the Directive, is towards the stringent and onerous.

2. Personal data

The Regulation, like the Directive, seeks to regulate the processing of information relating to identified or identifiable individuals (not legal persons), and is limited to data held in electronic form or in structured manual filing systems. Note, however, that the definition of "data subject" in article 4(1) resolves the debate as to what it means for a data subject to be "identifiable" in the broadest possible way, covering all circumstances where the data subject could be identified by ***any*** person, not just the controller. Thus, for example, IP addresses are likely to be treated as personal data, because an Internet Service Provider somewhere may be able to associate them with individuals. This raises the interesting question of how a controller's obligation to inform data subjects that it is processing personal data about them applies in circumstances where the controller cannot identify the data subjects. More widely, it appears that the common practice of encoding or redacting data before disclosure, so that the discloser can still identify the individuals to whom the data relate but the recipient cannot, for example where employee data are disclosed for due diligence purposes, will on the basis of the current draft no longer take the disclosed data outside the scope of data privacy law. The proposal is not clear in this respect, however, and it is to be hoped that it will be clarified in a more pragmatic direction.

Note that the proposed Regulation is more prescriptive than the Directive, in various respects, in relation to the processing of personal data relating to children (see for example article 8), and it introduces a harmonised definition of "child" which covers anyone under the age of 18, setting a more protective standard than the current regimes in various of the member states – although the express requirement to obtain the consent of a parent or custodian only arises if the child is below the age of 13 (article 8(1)).

3. Geographical scope

Under the current regime, EU data protection laws apply to processing carried out in the context of a controller's EU establishment or, where the controller is not established in the EU, carried out using means located within the EU. There had been a hope that the second limb of this regime might be removed as a disincentive to non-EU organisations outsourcing their processing to EU member states.

On the contrary, the proposed Regulation (article 3) ***extends*** the geographical scope of EU data protection law. The second limb of the Directive's regime is tweaked so that processing has to be carried out ***by a processor*** within the EU, rather than merely ***using means*** within the EU, to be caught, but additional and rather unclear provisions are included which will catch all processing related to the offering of goods or services to EU residents within the EU or the monitoring of the behaviour or EU residents, even if the controller and the processor are both located outside the EU - so, for example, it appears that CCTV systems in New York will be caught where they monitor the behaviour of EU residents on holiday, although this is not clear as the proposed Regulation's recitals suggest that it may be thinking only of monitoring of behaviour on the Internet. This will be highly controversial, particularly given EU data protection authorities' complaints as to the extra-territorial effect of, for example, US law.

4. The controller / processor distinction and obligations of processors

While the proposed Regulation (article 4) preserves the Directive's distinction between a "controller" (which determines the purposes for which, means by which and, under the Regulation, "conditions" on which personal data are processed) and a "processor" (which processes personal data on behalf of a controller), and also preserves and intensifies the controller's obligations when it selects and uses a processor (see point 12 below), it also imposes express obligations on processors in relation to matters such as keeping records of processing operations (article 28) and security (article 30). This "decides" an area of uncertainty under the Directive, where the UK implementation, for example, imposes essentially no direct obligations on processors while the implementations in other member states give processors varying degrees of data privacy compliance responsibility. It will be of concern to outsourced service providers, who typically argue in negotiation with their customers that they are not in a position to decide what level of security is "appropriate" to protect their customers' data – under the Regulation they will be responsible to data subjects for that decision, alongside the customer.

5. Legitimate processing

The proposed Regulation preserves the general approach of the Directive to the lawfulness of processing of personal data, starting from an absolute prohibition of the processing of personal data generally (article 6) and sensitive personal data in particular (article 9) and then moving on to identify the particular circumstances in which processing is permitted. The main change in relation to conditions for processing of personal data generally is an attempt to resolve the debate which has arisen under the Directive as to the circumstances in which it is necessary and/or appropriate to rely on ***consent*** to justify the processing of personal data. The so-called "legitimate interests condition", allowing a relatively wide range of processing without the need for consent, is preserved in the Regulation without material change or condition (article 6(1)(f)), hopefully sweeping aside the difficulties associated with reliance on this condition in many member states under the laws implementing the Directive. At the same time article 7, although rather cut down since the internal draft of the Regulation leaked towards the end of 2011, makes (fairly) clear that consent should only be relied upon in very limited circumstances. Consent must be "explicit" and certainly cannot be given by inertia; it can be withdrawn at any time, even if given by contract; and it is not effective where there is a significant imbalance between the position of the controller and the data subject. This last point is likely in practice to rule out reliance on consent in the employment context – and recital (34) to the proposal appears to confirm this, although article 7 itself is less categorical in this respect that in the leaked internal draft. Controllers are being guided towards reliance on legitimate interests where processing is not genuinely optional, which seems to us to be a sensible direction of travel.

It is to be regretted, on the other hand, that the Commission still considers it necessary to impose specific – and highly inflexible – rules as to the processing of personal data in the categories identified by article 9 as sensitive. The real sensitivity of personal data in these categories depends on the context in which they are processed – an entry in a clinical trial database, for example, is more sensitive than a statement in a business email that John Smith cannot attend a meeting because he has flu – and there is no reason why the general principles in article 6 could not adequately regulate processing of all

categories of data, Article 9 extends the sensitive categories so that they now explicitly include genetic data. In some member states, on the other hand, the Regulation is in this respect likely to have a minor relaxing effect, in that the new regime will clearly not apply to personal data revealing actual or alleged crimes (only actual convictions). It should be borne in mind however that, as discussed at 1 above, member states may introduce tighter restrictions in the employment context.

Various points in the proposed Regulation (e.g. Article 6(3)) confirm the view taken by the EU data protection authorities in relation to the interpretation of the Directive, that references to "law" in EU data privacy law (permitting controllers to do things which would otherwise be prohibited where they need to do so in order to comply with the "law") are to be read as applying only to the laws of the EU and the relevant member state and not to foreign laws. Controllers will, therefore, still on occasion be caught between processing and disclosure obligations under foreign law, on the one hand, and data privacy obligations under the Regulation, on the other. The proposed Regulation does nothing to address this dilemma.

6. Transparency

The Directive's transparency regime, requiring a controller to provide information to data subjects about its processing of their personal data, is preserved in the proposed Regulation (article 14 – and see also articles 19(2) and 20(4)). Unfortunately, however, it is also extended, so that information which under the Directive need only be provided where necessary to ensure that processing is fair will under the proposed Regulation have to be provided irrespective of considerations of fairness or, indeed, proportionality. This is already the case under the laws of some member states but it had been hoped that a harmonised approach might reduce the regulatory burden in this area. Where, for example, a controller collects the office contact details of an individual representative of a corporate supplier or customer for use in managing a business relationship, the controller will in theory be obliged to inform that individual of the period for which it will store those contact details; that he or she has rights of access, rectification or erasure and objection; that he or she can complain to a data protection authority, with contact details; and of various other items of information entirely inappropriate to the circumstances. As in many other areas, the Regulation appears in this respect to have been drafted as if it applied to a much narrower range of non-trivial processing than is in fact the case.

On the positive side, the exception to the transparency regime which arises under the Directive where personal data are not collected directly from the data subject and to contact and inform him or her would involve disproportionate effort, which has not been properly implemented, or has been implemented subject to cumbersome conditions, in some member states, is preserved, and member states have the opportunity to legislate to identify circumstances in which data subjects need not be informed of personal data collected indirectly if to inform them would "impair the rights and freedoms of others" (article 14(5)).

7. The right to be forgotten

The proposed Regulation's introduction of the so-called "right to be forgotten", set out in article 17, has been much anticipated and appears to be an important plank of the Commission's programme. It is not clear, however, what it adds to the provisions already included in the Directive and elsewhere in the proposed Regulation. Article 19 gives data subjects a right to require controllers to cease processing their personal data in circumstances where they are no longer legally entitled to process those data (for example, because the processing is justified by consent, which is then withdrawn). In these circumstances, however, controllers would under both the Directive and the proposed Regulation (articles 5(e) and 6(1)) be prohibited from continuing to process the data, irrespective of whether the data subject asks them to stop. It is therefore unclear what article 17 adds to the proposed Regulation, apart from an obscure provision in article 17(4)(a) requiring the controller to restrict the processing of personal data while it considers a data subject's claim that the data are inaccurate – we will need to await developments over the legislative process.

8. Data portability

The proposed Regulation introduces the concept of "data portability" in article 18. It is debatable whether data portability is a "data protection" issue at all, since it is aimed at allowing data subjects to make use of their personal data rather than seeking to protect their privacy. In our view data portability would be best addressed, if at all, on a careful sector-by-sector basis.

As it stands, the article is sweeping and potentially dangerous. It essentially expands the subject access right to allow data subjects to demand that they are given copies of their personal data in "an electronic and structured format which is commonly used and allows for further use by the data subject", wherever personal data are processed "by electronic means and in a structured and commonly used format"; and goes on, where the controller's processing is justified by consent or contract, to allow the data subject to transmit those data (although it is not entirely clear where), apparently irrespective of confidentiality and intellectual property issues. This appears to be thinking of data subjects downloading their data from one social network and passing them on to another, but it will also apply in a wide range of other circumstances in which the data subject's personal data will also be or include confidential or proprietary information of the controller – for example, a departing employee could in principle use this right to download and transfer to his or her new employer information about his or her role in the employer's business, over-riding the duty of confidence that he or she would otherwise owe and the employer's intellectual property rights in its own materials. This proposal is confused and unworkable in its current form and it is very much to be hoped that it will be deleted or substantially re-worked during the legislative process.

9. Other data subject rights

The data subjects' rights of access, rectification and objection, and the right to object to the use of automated-decision taking techniques (now re-branded as a right to object to "profiling") are all preserved and, in various respects, extended in the proposed Regulation (articles 15, 16, 19 and 20).

10. Formalities

The proposed Regulation does sweep away the Directive's "notification" regime, requiring controllers to register their processing of personal data with data protection authorities in all or most of the member states in which they are established. This, however, turns out to be little more than a pyrrhic victory for business. It should eliminate the need to complete many different forms to notify authorities in different member states, and it will be very helpful in member states such as France, where the notification procedure is so onerous as to be almost impossible to comply with in practice on a comprehensive basis, but it is replaced by requirements which may collectively turn out to be even more onerous:

- a requirement, applicable to processors as well as controllers, to maintain detailed "documentation" of processing operations, containing all the information required to be included in notifications made under the Directive, with the Commission having a power to stipulate standard forms for the maintenance of this documentation (article 28) – although controllers and processors with fewer than 250 employees (apparently per-entity, not across a group) will be exempt from this requirement;
- a requirement, also applicable to processors as well as controllers, to have in place an "independent" data protection officer, with security of tenure, who must meet specific conditions and fulfil various specific roles and whose identity must be notified to the data protection authority and to the public (articles 35 to 37) – this is based on the current German model, although there is, again, a relatively helpful exception for private sector controllers or processors with fewer than 250 employees unless their core activities involve regular and systematic monitoring of data subjects; and
- a requirement to consult a data protection authority in relation to processing which is likely to present "specific" risks –processing will be deemed to present specific risks if a data privacy impact assessment indicates that it may (see point 11 below) or it is in a category set out in a list published by the data protection authority for this purpose (article 34, raising the possibility that some authorities may publish very long lists); and the data protection authority will have the power to prohibit the processing, and it appears (although it is not clear) that the processing will not be able to go ahead until the authority has confirmed that it does not oppose it.

The proposed Regulation also preserves the Directive's requirement that controllers which are not established in the EU should appoint local representatives for data protection purposes (article 25), although it does provide helpful exceptions (for example, where the controller is established in an "adequate" jurisdiction such as Switzerland or has fewer than 250 employees). The proposed Regulation also resolves the question, left open by the Directive,

of whether appointed representatives are responsible for the compliance failures of their appointing controllers: all penalties under the Regulation are to be imposed on the representative (article 78(2)).

Removal of the registration regime raises the question of how the activities of those data protection authorities which are currently funded by registration fees will be funded when the proposed Regulation comes into effect – the obvious options being through fines (see point 14 below) or out of general taxation.

11. The new data protection "nanny state": privacy by design, impact assessments, etc.

One of the aspects of the proposed Regulation which is likely to prove most unpalatable to businesses – and particularly to businesses for whom the processing of personal data is not a core part of their operations – is the abandonment of the Directive's relatively clean, principles-based approach to data protection. The proposed Regulation preserves and expands on all of the data protection principles set out in the Directive, but it also imposes a set of rules regarding the steps that controllers should take to comply with those principles, irrespective (for the most part) of the nature of the processing that they carry out. Again, there is an assumption that all regulated processing is important processing in relation to which costly compliance steps need to be taken.

We have already discussed the new requirements in relation to the appointment and role of internal data protection officers and the documentation of processing. The proposed Regulation will also, for example, require controllers to:

- have in place "transparent and easily accessible" data protection policies (article 11(1));
- have in place internal procedures and mechanisms for responding to the exercise of the data subject rights discussed at points 7 to 9 above (even if, as will often be the case, the controller has never in practice received a request to exercise those rights and does not expect such requests in the future) (article 12);
- design their internal technical and organisational measures and procedures with a view to compliance with the Regulation and, in particular, implement measures to avoid collection of unnecessary personal data, over-retention of personal data and personal data being accessible to an indefinite number of individuals (article 23); and
- in vaguely defined circumstances (where processing operations "present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes"), carry out data privacy impact assessments, including consulting data subjects or their representatives (article 33).

Note that the risks presented by a processing operation to give rise to a requirement for an impact assessment must only be "specific", not necessarily ***serious*** or ***likely to materialise***. Article 33(2) gives a non-exhaustive list of examples of processing posing specific risks. This list is unhelpful in itself, because it will require impact assessments to be carried out where proposed processing operations fall within the identified categories irrespective of their practical significance in context, which may be very low. The items included in the list do, however, suggest that the proposed Regulation is intending to catch only relatively "risky" processing operations. This is to be contrasted with article 30(2), which suggests that ***all*** processing, however innocuous, must be subject to an "evaluation" of the data security arrangements in place to protect the data,

These provisions might helpfully be refined in the on-going drafting process.

12. Security and breach notification

Data security is, of course, a hot topic, and one of the few respects in which the US can for the moment claim to have a more rigorous data privacy regime than the EU. It is perhaps unsurprising, therefore, that the proposed Regulation establishes a more onerous data security regime than the Directive. In particular, it:

- introduces a European "security breach notification" regime, which will require controllers to notify a data protection authority of any personal data breach (incredibly broadly defined, e.g. including each lost Blackberry), usually within 24 hours of the breach; and to inform data subjects of personal data breaches that are likely adversely to affect their personal data or privacy, subject to limited exceptions;
- imposes more specific and onerous requirements as to the terms on which a processor is appointed to process personal data on behalf of the

controller, including an unworkable requirement that the controller should always have an absolute right of veto over sub-contracting (article 26(1)); and

– allows the Commission to impose more specific security requirements (article 30(4)).

In practice, these requirements are likely to exacerbate the unfortunate process through which services contracts have in recent years gradually been overwhelmed by lengthy data security provisions out of all proportion to the importance of data privacy to the transaction; to flood data protection authorities with reports of trivial data security breaches; and to make security breach notifications to data subjects so frequent and so standardised that they are valueless. It is to be hoped that they will be re-visited during the legislative process.

13. International data transfer

There was hope that the new Regulation might radically reform the Directive's cumbersome approach to the international transfer of personal data, replacing the starting point of absolute prohibition, for fear that personal data may be abused if held outside the EEA, with a permissive regime allowing for prohibition on a case-by-case basis where particular risks are identified. So far, at least, this hope has unfortunately come to nothing.

The proposed Regulation does, however, liberalise the regime in some key respects:

– It "institutionalises" the concept of binding corporate rules (article 43), expanding the concept so that binding corporate rules can be put in place by processors as well as controllers and requiring data protection authorities to approve them provided they meet fairly limited criteria. These criteria are, however, subject to further specification by the Commission; and authorities will be obliged to inform each other authorities and the Commission, all of whom have a right to object, before approving a given set of rules. This should address some of the specific legal problems with binding corporate rules in some member states, and it may marginally reduce the log jam of applications for approval under consideration by the authorities, but it does not amount to a fundamental change of approach. The fact remains that binding corporate rules package will still be subject to approval by under-resourced data protection authorities and can therefore never represent a proper scalable solution to the international transfer problem.

– It prevents particular data protection authorities from reserving the right to approve (or dis-approve) transfers made on the basis of the European Commission's standard contractual clauses. Assuming that the Commission leaves in place the current standard forms this is likely to amount to a more fundamental change. Despite the limitations of the standard clauses, where controllers can use them across the EEA without seeking approval they are likely to do so, applying them through creative drafting to a very wide range of intra- and extra-group transfers of personal data and abandoning their labour-intensive binding corporate rules programmes. It is possible, of course, that the Commission may also look to refresh the standard clauses to take account of the changes introduced by the Regulation, and this may lead to further complications.

– It introduces a very limited "legitimate interests" condition to justify the transfer of personal data to "inadequate" jurisdictions (article 44(1)(h)). This, however, is limited to transfers which "cannot be qualified as frequent or massive", and depends on the transferor having assessed all the circumstances and adduced appropriate safeguards to protect the transferred data. It is unlikely, therefore, that it will be capable of widespread use in practice.

On the other hand, the proposal makes clear (article 41) that only the Commission, and not a controller, can decide that a particular jurisdiction ensures an adequate level of protection for personal data. This question was left open under the Directive and different member states have taken different approaches. In the UK, for example, controllers quite frequently take the view that a transfer can be made to a non-EEA ***processor*** without the need to a contract in the appropriate Commission standard form, on the basis that the jurisdiction in which the processor is located can reasonably be taken to ensure an adequate level of protection for personal data which remain protected by UK data protection law because they are processed in the context of the transferor's UK establishment. This will not be possible under the Regulation as drafted.

14. Enforcement / sanctions

The Directive leaves enforcement and sanctions essentially to the discretion of the member states, and practice varies considerably. It is probably fair to say that the EU data protection regime has a reputation for being onerous, on the one hand, but rather toothless, on the other. Its toothlessness to some extent stems from the data protection authorities' lack of resources, and there is nothing in the proposed Regulation to address this issue. It does, however, seek to ensure that tough sanctions are available to punish compliance failures. In particular:

- Data protection authorities will retain their existing right to order compliance, and they will have statutory audit rights (not available under the current regime in all member states) (article 53).
- Data subjects will retain their existing right to civil damages for breach of the Regulation (article 75) and will now be able to exercise those rights against processors as well as controllers. Rights to compensation will now extend to anyone affected by a breach, even if they are not individuals (article 77),
- Specific administrative penalties for breach of the Regulation are to be enacted at member state level (article 78). Data protection authorities will also have the power (and duty) to impose administrative fines under the Regulation, however, and these could reach very high levels. In particular:
  - intentional or negligent failure to comply with some requirements regarding data subject rights (see points 7 to 9 above) will attract a fine of up to 0.5% of annual worldwide turnover;
  - intentional or negligent failure to comply with some other requirements (including, for example, the transparency requirements (see point 6 above), some other requirements regarding data subject rights and the requirement to document the processing of personal data (point 10)) will attract a fine of up to 1% of annual worldwide turnover; and
  - intentional or negligent failure to comply with most of the key requirements of the Regulation (including, for example, the legitimate processing requirements (point 5), most of the "nanny state" requirements (point 11) and the data security (point 12) and international transfer (point 13) requirements) will attract a fine of up to 2% of annual worldwide turnover.

  Below these limits, the level of the fines is supposed to be set so as to be proportionate to the seriousness of the breach,

  Setting limits by reference to global turnover is an extremely blunt instrument in this context – a global concrete manufacturer, for example, could be exposed to the same level of fine as a global retail bank of similar size. Note, however, that the references to "turnover" are to the turnover of the "enterprise", which appears to mean the specific legal entity concerned rather than the consolidated group; and that there is the alternative of a written warning without sanction in the case of an employee with fewer than 250 employees which processes personal data only as an "ancillary" activity.

  Generally, very serious sanctions for breach, capable of being imposed immediately rather than only where a controller fails to comply with instructions received from a data protection authority in response to a breach, and combined with substantive requirements which are even more onerous than those of the Directive, are likely to lead to disproportionate attention and resources being devoted to data protection compliance issues, particularly where personal data are processed in innocuous ways unlikely to cause any harm. Controllers will not be able to assume that authorities will exercise their discretion in a proportionate fashion when they come to enforce.

  Note further that data protection authorities will not generally have the option to decide ***not*** to levy a fine in respect of a relatively minor breach.

The proposed Regulation's rules as to jurisdictional competence as between the member states and their data protection authorities are not entirely clear. Article 51 provides for a given data protection authority to enforce the Regulation against a given controller or processor if its main establishment is in that authority's member state, introducing a limited degree of home country regulation (or at least regulatory enforcement). This does not apply across groups of entities, however, so it will remain the case that, for example, the UK subsidiary of a French parent will be regulated by the UK rather than the French

data protection authority – one exception being in relation to binding corporate rules, where it appears that a group of companies will be able to make an application to a single authority. No clear rule is provided as to which data protection authority should take responsibility for enforcing the Regulation against controllers and processors established outside the EEA, but presumably they will be expected to enforce according to the member states in which representatives are or should have been appointed (see point 10 above). The proposal does not stipulate which national courts will be competent to hear disputes in relation to processing governed by the Regulation. Generally, this is an area which would benefit from a clearer regime if the Regulation is to be enforced in practice.

The road to implementation

The Commission's proposal will now be passed to the European Parliament and the Council of the European Union for amendment and adoption following the ordinary EU legislative procedure. This will give clients an opportunity to lobby MEPs and member state representatives in the Council, and indeed the Commission itself, to press for changes in the text of the Regulation. Assuming that an agreement can be reached, the Regulation will eventually be published in the Official Journal. If published in its current form it will come into force 20 days later but will not "apply" (and clients will not, therefore, be obliged to abide by it) for a further two years. In practice, therefore, it is likely to be at least three years, and probably rather longer, before the Regulation takes effect.

Clifford Chance's Global Data Privacy and Management Group

Clifford Chance' operates a global data privacy and management group, co-ordinated by Richard Jones, the firm's Director of Data Privacy. The group exists principally to help Clifford Chance's clients keep on top of the complex network of legal and regulatory issues affecting the management of data across global or regional organisations. Organisations operating to a significant degree as single businesses across multiple jurisdictions need to develop coherent strategies to address the many and complex issues that arise in this area. Clifford Chance's focus is on the delivery of practical strategic advice which takes full account of local issues but seeks to deliver global solutions wherever possible. We use our extensive experience to provide streamlined and practical advice, anticipating issues at an early stage in each project to the extent possible and controlling cost.

The group has a very wide range of experience, going back to the early 1990's. It includes data privacy, employment, regulatory and other lawyers across our global network and regularly works with colleagues in other firms, in countries where we do not have a presence, who participate in our multi-jurisdictional teams to advise on their local laws.

If you would like to know more about the group, please contact one of the lawyers set out opposite or your usual Clifford Chance contact.

Contacts

Richard Jones
UK / group co-ordinator
E: richard.jones@cliffordchance.com
+44 (0)20 7006 8238

Bart Vanderstraete
Belgium
E: bart.vanderstraete@cliffordchance.com
+32 2533 5908

Victoriano Melero
France
E: victoriano.melero@cliffordchance.com
+33 14405 5282

Marc L. Holtorf
Germany
E: marc.holtorf@cliffordchance.com
+49 89 21632 8471

Claudio Cerabolini
Italy
E: claudio.cerabolini@cliffordchance.com
+39 028063 4248

Ruth van Andel
The Netherlands
E: ruth.vanandel@cliffordchance.com
+31 20711 9268

Marcin Czarnecki
Poland
E: marcin.czarnecki@cliffordchance.com
+48 22429 9412

Sonia Sebe
Spain
E: sonia.sebe@cliffordchance.com
+34 93344 2208