PAUL | TICHER

Briefing: The proposed new EU Data Protection regime, January 2013

Background

For several years it has become apparent that the present EU Data Protection regime requires updating. Having been drawn up in the 1990s, it cannot adequately deal with technological developments that have taken place since then – such as cloud computing and social media.

On 25th January 2012, therefore, the EU Commissioner responsible for this area, Viviane Reding, put out proposals for a complete overhaul of the Data Protection regime. These proposals are in the form of a Regulation which would completely replace the current Directive (95/46/EC) and its associated national legislation in each of the 27 member countries.

The difference between a Regulation and a Directive is that a Regulation is, in effect, a single law that applies across the EU. A Directive sets out rules that each EU member state has to 'transpose' into national legislation. The result can be significant differences between different countries, or even inadequate implementation of the Directive; indeed the European Commission holds the current UK legislation to be deficient in a number of key areas.

This paper picks out some key issues and changes that the proposal would make to the current situation, in particular those that have significance for voluntary organisations, and also looks at some of the responses to the proposal since it was published.

Note that, to avoid repetition, the Regulation and its provisions are not consistently described as 'proposed' in the discussion below.

Regulation or Directive?

The UK government has from the start objected consistently and vehemently to a Regulation, preferring the "greater member state flexibility" inherent in a Directive, which could give "due regard to national tradition and practice". This objection probably stems partly from the UK government's distaste for some aspects of the Regulation, and EU regulation in general, but could also mean that they would prefer just to make the minimum number of amendments to our existing legislation, rather than replacing it with a completely new measure.

If the UK government were to succeed in its aim of renegotiating its relationship with the EU, this could of course be one area on which powers might be "returned" to the UK.

In November 2012 it was reported that there were nine states in favour of a Regulation, five for a Directive and 13 undecided. The Regulation needs a three quarters majority to go through, so it could be blocked if just a few more states come out against.

One other point to note is that the Regulation specifically excludes police and national security data processing. There is a parallel proposed Directive to cover these areas which – since it is a Directive – would leave a lot more scope for each state to bring in its own flavour of the rules. The Regulation also excludes processing carried out by the EU itself.

Progress so far

The Proposal was published in January 2012. Since then, the Information Commissioner, the UK government (and of course other governments) and EU institutions have been able to comment, with hundreds of amendments put forward. Some are quite small and probably uncontroversial, but others are pretty fundamental. This means that while the issues are now becoming much clearer, the final form of the new regime is uncertain.

In each section below, the changes proposed are summarised in **bold**. The *italics* report relevant comments from the Information Commissioner and others, including my explanation of selected issues and brief opinions (in blue). At the end of each section is a box with my summary of the probable implications for UK voluntary organisations.

Enhanced individual rights

The Regulation would have the effect of significantly enhancing individual rights. The detail is given below; the main themes are:

- In some situations people and their data would be covered by the Regulation where at present they are either not covered or the position is unclear.
- Consent is required in more situations, and has to be more definite. 'Soft' consent (see below) would be a possibility in far fewer cases, if any.
- Data Subjects must be given more and clearer information as a matter of course by the Data Controller.
- There are new Data Subject rights such as a 'right to be forgotten' (in limited circumstances) and a right of 'data portability' when the Data Subject wants to move from one provider to another.

Definition of the Data Subject & Personal Data

The definition of 'Data Subject' is extended to include 'online identifiers', such as IP addresses, pseudonymous usernames and profiling information. However, if the Data Controller can't identify the real person, they don't have to seek additional information to identify them if, for example, they get a Subject Access Request.

> *This would have to be taken into account where people are able to sign up for services using nicknames, or where the system allocates them some kind of identifier, even if their real details are not captured.*
>
> *The Information Commissioner feels that further clarification is needed, and would like the provision to mean that a person can be 'identifiable' if the online identifiers are used to target advertising or treat the person differently from other people, even if their true identity is not known to the Data Controller. The European Parliament has also commented in similar vein.*
>
> *This seems to be heading in the direction of a useful clarification, but the Information Commissioner's points are well made.*

The Regulation aims to apply in situations where Data Subjects are within the EU but the Data Controller is outside, if the processing relates to offering goods or services or monitoring online behaviour.

> *The Information Commissioner is sceptical about how this could be enforced. The provision is unlikely to affect many UK voluntary organisations, but could*

possibly have an effect in some cases where organisations in the UK are working alongside – and sharing information with – organisations overseas. Where the new rule applies, the UK organisation may find itself having to act as 'representative' of the overseas organisation, and to bear some responsibility for the overseas organisation's processing of data about EU Data Subjects.

The Information Commissioner must be right on this one.

The definition of Personal Data repeats Directive 95/46/EC, referring to "any information relating to a Data Subject".

*In the UK, legal decisions (principally the 'Durant' case in 2003) have narrowed the definition, concluding that the data has to be **about** the individual and affect them in some way. Implementation of the new provisions as a Regulation could well remove this restriction.*

This would not completely resolve the uncertainty around the fringes as to what counts as Personal Data in the UK (e-mail addresses on their own being a good example), but might help.

Most UK voluntary organisations are already careful in how they treat borderline information. In most cases, therefore, these changes would bring clarity rather than requiring a significant change of practice.

Consent

The UK government considers that the provisions on consent would be "cumbersome" and disturb the online experience of users.

The Information Commissioner argues that if consent is made harder to obtain, Data Controllers must be given alternative ways to make their processing legitimate when it is low risk and uncontroversial.

The distinction between 'consent' and 'explicit consent' is removed. The Regulation defines consent as: "any freely given, specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".

The difference here is the requirement for 'a statement ... or clear affirmative action'. 'Soft consent' – i.e. approaches such as assuming that people consent if they carry on using a service, or giving them a pre-ticked consent box – may no longer be possible.

At the same time the Regulation tightens up on the marketing opt out. The onus is currently on the Data Subject to object; under the Regulation the opt-out must be "explicitly offered ... in an intelligible manner".

The Data Controller would bear the burden of proof on consent. Written consent for processing must be distinct from associated consent for other matters.

Cumulatively, these changes make 'soft' consent much harder for the Data Controller to obtain although they do not necessarily mean the end of all approaches that use an opt out. The Information Commissioner is generally in favour but has doubts about some aspects. For example, he argues that some types of consent (e.g. for medical treatment) should imply consent for processing the associated data.

Although these provisions may cause a few problems for organisations, on balance it seems right to make sure that consent really does mean consent.

There is explicit clarification that the Data Subject can withdraw consent. For obvious reasons this cannot take effect retrospectively.

Consent would no longer be valid if there is a "significant imbalance between the position of the data subject and the data controller".

This provision is apparently intended to prevent employers making consent a condition in their employment contracts. The Information Commissioner argues that some employer/employee consents (e.g. next of kin details) are valid, notwithstanding the imbalance, since the provision is optional and there is no detriment for failing to consent.

This would reinforce the move towards making consent more genuine.

An interesting question is the extent to which this provision would cover other non-negotiable terms & conditions, such as those that have to be accepted before a service is delivered on line.

These provisions are likely to require a thorough review of what options are offered and how they are presented, particularly in relation to fundraising and other marketing.

Transparency

Data Controllers will have to have transparent and easily accessible policies, written in plain English, and adapted to the Data Subject, especially children.

The Information Commissioner welcomes this, saying that "privacy policies, couched in difficult legal language, [have] often become exercises in corporate indemnification, rather than being genuinely informative to the public".

This really should go without saying.

When they collect information from people, Data Controllers will have to provide more information than the current minimum – including the length of time for which data will be held, and whether the data being requested is obligatory or voluntary.

The Information Commissioner wants to see a distinction between:

- *Information that is obligatory because it is required by law;*
- *Information that is obligatory because the service being requested cannot otherwise be provided; and*
- *Information that the Data Controller has decided will be obligatory.*

The Information Commissioner's suggestions are very helpful.

Data Controllers will have to tell people where they got their data from, if not directly from the Data Subject.

Many organisations still have work to do on their policies – especially once they have to be written in plain English – and many statements on websites and forms will have to be revised to include the additional information required.

Other Data Subject rights

Time limits and procedures for providing information and for complying with Data Subject rights are specified in more detail, and charging for Subject Access is not permitted.

> *The Information Commissioner and the UK government think that the option to charge for Subject Access should continue, as a deterrent to frivolous requests.*
>
> *There is some merit in the argument that a modest charge is appropriate.*

There is a new right of 'data portability', so that individuals can get a copy of their data in electronic form and in a standard format if they want to change service provider.

> *The Information Commissioner sees some practical difficulties with this concept.*

When a Data Subject does not want a Data Controller to process their data, the burden of proof will change, so that it will be up to the Data Controller to justify why the data should be processed rather than, as now, for the Data Subject to justify why it should not.

> *This would be a useful enhancement, even though it would only affect a small number of cases.*

There are a set of additional restrictions on automated profiling.

> *The Information Commissioner generally welcomes the idea but wants to see more of a risk-based approach.*

See also the 'right to be forgotten', below.

These new rights are important, but it remains to be seen how far they will affect voluntary organisations. Quite possibly the impact will be slight.

Technological developments

Partly in response to problems that people have had in getting embarrassing information deleted from social media sites, the Regulation introduces a 'right to be forgotten'. This is obviously not absolute; there would be many instances where the individual would not be able to insist on data being removed completely.

> *The Information Commissioner thinks that this is an important provision, but the full implications have not been thought through. The UK government and many other commentators also fear that it is unrealistic.*

When data is wrong, or removed under the 'right to be forgotten', a Data Controller will have to notify anyone the data has been shared with about the correction or removal.

> *The 'right to be forgotten' could be controversial, but the rationale is clear.*

Processing data of a child under 13, in respect of 'information society services', should require parental consent, verified as far as possible.

> *This appears to be aimed mainly at ensuring that children cannot sign up to online services without their parents' knowledge*
>
> *The Information Commissioner apparently doesn't see the point of this (and wonders why the definition of 'child' elsewhere uses a different age limit). The reasoning for this is not clear.*

More pertinently, the Information Commissioner points out the difficulty of getting "verifiable parental consent", saying: "The ingenuity of children in circumventing age verification systems should not be underestimated."

Again, this is a reasonable objective, but probably hard to achieve in practice.

In a measure similar to the current UK 'domestic purposes' exemption, the Regulation exempts from the rules, processing "by a natural person without any gainful interest in the course of its own exclusively personal or household activity".

The Information Commissioner doesn't think this goes quite far enough. For example, it would be useful to make it clear that selling one's own possessions on eBay would be exempt, even though there is 'gainful interest'. This view has been supported by the European parliament.

Another concern is that the Regulation doesn't make it sufficiently clear how far providers of social media platforms are responsible (or not) for the content they host.

Voluntary organisations that make use of social media – and ones that support children in particular – will have to consider the implications of the eventual changes in this area.

Data Controller & Data Processor

The definition of Data Controller follows Directive 95/46/EC in making it clear that any kind of organisation can be a Data Controller.

The UK's current legislation has caused difficulties in knowing for sure whether some small charities are Data Controllers or not, since our Act defines the Data Controller as a 'person' – which can include companies but not unincorporated bodies. This appears to be a defective implementation of Directive 95/46/EC but the Information Commissioner has in practice followed the Directive rather than the letter of the Data Protection Act. If the outcome of the current process is a Regulation, the full definition will automatically apply in the UK.

A Data Controller must be able to demonstrate that they have policies and procedures in place to comply with the Regulation. These policies and procedures are then spelled out in some detail. The Regulation also sets out a list of specific documentation that the Data Controller has to maintain.

The Information Commissioner agrees that Data Controllers are likely to need policies, procedures and documentation, but feels that the Regulation is too prescriptive. It would be wrong to take enforcement action against a Data Controller just for not having the specified paperwork even if no individuals were actually at risk or if different paperwork was actually more appropriate. However, if something goes wrong and the Data Controller doesn't have any suitable policies and procedures that could be taken into account.

This set of provisions is one of the main objections of the UK government to the Regulation, arguing that it would impose an unnecessary and expensive burden on business, for no great benefit in terms of protecting individuals.

In response, the EU Commissioner has indicated that she would be prepared to negotiate on ways to reduce the perceived administrative burdens.

The Regulation includes a requirement to appoint an independent Data Protection Officer, with specified tasks, if the organisation is a public body, or employs more than 250 staff, or carries out monitoring of individuals as a 'core activity'.

> *The Information Commissioner raises a number of practical and theoretical issues with this and would like to see it dropped in its current form, while the UK government would prefer the nature of processing to be the determining factor.*
>
> *The requirements for a large amount of specific paperwork and for mandatory appointment of a Data Protection Officer do appear over-prescriptive and very bureaucratic. In their present form, these provisions would be disproportionate for many voluntary organisations.*

Provisions for registering with (or "Notifying") the national supervisory authority are completely absent from the Regulation. Instead, the authority has greater powers to find out what is going on if they need to – for example by asking to see the documentation referred to above. All the information currently included in the registration process (and more) is included in the set of required documentation.

> *The Information Commissioner has commented that supervisory authorities (such as the Information Commissioner's Office) need proper resourcing. It is not clear how the ICO would be funded in the absence of a Notification fee.*
>
> *On the other hand it is hard to discern much benefit from the current Notification procedure (apart from ensuring that the Information Commissioner gets some income independently of the government).*

There are provisions in the Regulation for the notification of all "personal data breaches" to the supervisory authority (in the UK, the Information Commissioner). Where the breach would "adversely affect the protection of the personal data or privacy of the Data Subject", the Data Subject must also be notified.

> *The Information Commissioner is understandably concerned about being swamped with reports of minor breaches, and would like to see 'triggers', to define when the breach is serious enough for it to be necessary to inform the supervisory authority and/or the Data Subject(s) affected. The UK government is concerned that there could be "subject notification fatigue".*
>
> *Mandatory notification of all breaches does appear excessive.*

The possible penalties for Data Protection breaches in the Regulation are fines of up to €1 million or 2% of company turnover.

> *The Information Commissioner and the UK government are unhappy that the Regulation links the level of fine to the size of the organisation rather than the severity of the consequences for Data Subjects.*

The Regulation imposes an obligation on joint Controllers to have an 'arrangement' determining their respective Data Protection responsibilities.

> *Joint Data Controllers are envisaged in Directive 95/46/EC but not discussed at all. As more and more collaborative work takes place, data sharing agreements have become commonplace, and the Regulation recognises this. It does not, however, prescribe the form or content of the 'arrangement' envisaged.*

The Regulation specifies in more detail than Directive 95/46/EC what must be in the contract between a Data Controller and a Data Processor (much of which is already recognised as good practice). It includes requirements for the Data Processor to:

- act only on instructions from the Data Controller;
- impose a confidentiality obligation on their staff;
- have adequate security (for which they are to be directly responsible, not just by virtue of their contract with the Data Controller);
- not subcontract work without the Data Controller's permission;
- hand over "all results" of processing to the Data Controller when their work is finished and not process the data further.

This is one area where major changes can be expected before the Regulation is finalised. However, whatever the outcome, many voluntary organisations are likely to have to make their Data Protection process more formal, and to have clear procedures for, if necessary, notifying any breaches that occur. Many contracts with Data Processors will have to be reviewed and probably amended.

Other things

The Regulation defines a 'child' to be under 18. It also makes it harder to process information about children on the basis of the Data Controller's 'legitimate interests' alone.

> *See also the separate provision discussed above to protect children under 13 who use online services.*

The Regulation does not clear up the confusion over the definition of a manual 'filing system'.

> *The Information Commissioner suggests that it would be more useful if the definition was based on the nature of the information, rather than the form in which it is kept.*
>
> *This suggestion would be a significant improvement on the current situation.*

The Regulation does not resolve difficulties over what the UK terms 'sensitive data', and may make matters worse by replacing the term 'religious or philosophical beliefs' in Directive 95/46/EC with the term 'religion or beliefs', which could well be open to too-wide an interpretation.

> *The Information Commissioner points out that – among many problems with this part of the current legislation – people in different countries are 'sensitive' about different types of information.*
>
> *The rules on 'sensitive data' under the present legislation are confusing and unhelpful. They manage to prohibit manifestly reasonable activities that do not adversely affect the individual. The Regulation would be more helpful if it took more of a risk-based approach here, or at least had a more flexible list of suitable conditions under which 'sensitive' data may be processed.*

There are numerous provisions where the Commission "may" lay down standard forms for this and that.

A considerable part of the Regulation deals with the powers and activities of the national supervisory authorities and the setting up of a central European Data Protection Board (to supersede the existing 'Article 29 Working Party' but with far greater powers). There are also measures aimed at getting greater consistency and cooperation across the European Union.

> *These two areas lead to a fundamental objection of the UK government, and one of their main reasons for preferring a Directive over a Regulation. A Directive would not be able to give so many additional powers to European-level institutions and activities. Many other governments are also unhappy with the increased powers at the European level, and the Commissioner proposing the Regulation has already said that she would be prepared to take out 40% of the provisions for the European Commission to set rules directly. The European parliament has also supported reducing the Commission's powers in this area.*

The Regulation revises the provisions for overseas transfers significantly.

> *The Information Commissioner thinks it's still wrong.*
>
> *He's right. In particular, it does not seem that there is much in the Regulation to solve the problems of using cloud services.*

Most of these provisions are unlikely to affect voluntary organisations significantly, unless cloud computing ends up with major restrictions.

What happens next?

Most of the changes to individual rights – possibly apart from the tightening up on marketing consent – and those responding to technical developments, appear to be ones that many voluntary organisations would support even if it means a flurry of additional work to get fully up to new standards. In many cases voluntary organisations will have little difficulty in complying, as their practice often goes beyond the current minimum requirement. There is therefore no need for action at this point.

The proposals on Data Controller procedures would be burdensome if they are not changed, but they are unlikely to remain in their present form, given the extent of opposition.

It is expected that some key decisions will be taken by the EU Council of Ministers in the summer of 2013. Unless they completely fail to get agreement and revise the timetable, any remaining issues should then be ironed out by the end of 2013. A Regulation would then come into force almost straight away (but presumably with a transition period). A Directive, on the other hand would then require domestic legislation, probably taking up to five more years if the experience with Directive 95/46/EC is anything to go by.

Resources

The text of the proposed Regulation can be found here:
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

The Information Commissioner's detailed initial look at the proposal is here:
http://www.ico.gov.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx