Proposed new EU General Data Protection Regulation:

Article-by-article analysis paper

V1.0 12 February 2013

About this document

We originally produced this document for two main audiences – the ICO's own staff and the Ministry of Justice, to help to inform the UK's negotiations in Europe. However, it has become clear that the information contained in this paper could be of use more widely, as a resource for all those with an interest in the data protection reform process and the ICO's views. Therefore we have decided to publish it.

This document supplements the initial analysis paper on the European Commission's legislative proposals that we published in February 2012. We have had no reason to deviate from the general lines we set out then – which we think are still basically right - but we are in a better position now to set out in more detail our views of the substantive provisions of the proposed Regulation. In particular, we have drawn on expertise from across the ICO to develop a much clearer understanding of the practical implications of the European Commission's proposals as they stand.

This paper contains comprehensive and detailed analysis of most of the Articles of the Regulation. Where we do not comment on a particular Article, this means we are content or have not formulated a view yet. This paper necessarily focuses on areas of uncertainty or issues that we have reservations about.

We will update this paper from time to time, to add content and to revise our analysis as events in Europe progress and our own understanding develops.

The ICO cannot table amendments or formally propose alternatives to the wording in the proposed Regulation. However, we hope that the analysis contained in this paper will help MEP's and others to do so.

Article 1
Subject matter and objectives

1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

ICO comment: This makes it clear that despite the many changes and additions, the basic concepts and the overarching purpose of data protection law remain essentially the same. This provides important continuity with current data protection law.

Article 2
Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;
(b) by the Union institutions, bodies, offices and agencies;
(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;
(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;
(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

ICO comment: It should be made clear that, in some contexts, processing personal data for gainful interest can still be in the course of a person's exclusively personal or household activity, for example, when someone sets up a website to sell on their unwanted birthday presents.

We would prefer wording such as 'in pursuit of a commercial objective', whilst noting that some non-gainful activity – such as running a political campaign – can be non-personal.

There has been some suggestion the Regulation should be used to 'implement' the Lindqvist decision – in short meaning that information posted openly on the internet necessarily falls outside the law's personal or household processing exemption. We never wholly accepted the reasoning in Lindqvist and do not accept that there is any need to 'implement' it through the new Regulation. However, we have accepted the view that the open publication – or not – of personal data might be one factor to be taken into account when deciding whether or not processing is being done for personal or household purposes. We certainly think the law should provide better criteria for doing this, as our experience suggests that it is becoming increasingly difficult to determine whether or not processing is being done for personal or household purposes. The current intention is that there will be a Regulation for most data controllers but a Directive for crime prevention etc. bodies. We would prefer a single instrument across the piece but, however it works out, we want to see as much consistency as possible across the piece. We cannot see the case for the Directive being weaker than the Regulation.

Article 3
Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

ICO comment: Clarification is needed as to how paragraph (2) will work in practice. We like the idea of Member States' citizens having the same data protection rights whether they are dealing with an EU or non-EU controller. However, we have real doubts as to how enforceable this will be, for example when we try to get a Brazilian company to grant subject access rights to an individual or to cease marketing to him or her. As a general theme, we do not want citizens to be given the impression that they have a level of protection that cannot be enforced in practice.

The issue of 'monitoring' is proving problematic. We had assumed that 2(b) was aimed at international electronic service providers – e.g. US companies – that use behavioural profiling to target ads and other content at EU citizens using their services. However, there has been some debate recently as to whether this kind of activity is meant to be covered by this provision. We need greater clarity as to what is meant by 'monitoring' and how 'anti-monitoring' rights will be enforced in practice when non-EU organisations are carrying it out.

Article 4
Definitions

For the purposes of this Regulation:
(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
(2) 'personal data' means any information relating to a data subject;
(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;
(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;
(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;
(8) 'the data subject's consent' means 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;
(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

disclosure of, or access to, personal data transmitted, stored or otherwise processed;
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;
(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;
(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;
(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;
(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;
(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;
(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;
(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;
(18) 'child' means any person below the age of 18 years;
(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.

ICO comment: The main issue for us here is about scope. The definition of personal data is essentially a reorganised form of the current Directive's definition. That is good in terms of continuity.

However, there is clearly considerable debate about whether certain forms of information are personal data or not. This is particularly the case with individual-level but non-identifiable - or not obviously identifiable

data - such as is found in a pseudonymised database. We prefer a wide definition of personal data, including pseudonymised data, provided the rules of data protection are applied realistically, for example security requirements but not subject access. If there is to be a narrower definition it is important that it does not exclude information from which an individual can be identified from its scope. However, it is important to be clear that a wide definition plus all the associated rules in full would not work in practice. This is a real issue in contexts as diverse as medical research and online content delivery.

While we welcome the high standard of consent in Article 4 (8), it is important that the strengthening of consent does not leave data controllers without a lawful basis for processing which is either necessary or unobjectionable. Usually, there need to be alternatives to consent.

Ideally, we would like to see a 'fix' to the issue of non-automated filing systems. This has proved problematic over the years, particularly because almost all filing systems are structured in some way – if only in a simple chronological manner – but this does not mean that it is easy – or even possible – to locate information about particular individuals.

Article 5
Principles relating to personal data processing

Personal data must be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;
(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;
(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

ICO comment: We welcome the general continuity with the existing Principles here. We also welcome the recognition of data minimisation principles provided for in (c) and also that responsibility and liability for ensuring and demonstrating compliance is placed firmly with organisations in (f). This updates the Principles well and gives a clear statutory basis for the data minimisation principles the ICO has been promoting as good practice for many years.

It is worth giving some thought to the distinction between the lawfulness and transparency provisions in (a) and the purpose limitation ones in (b). It is worth noting that in other Member States, 'fairness' is primarily about transparency and not about fairness of use – which is generally treated as more of an 'incompatibility' issue. It is worth considering how it 'fairness' will be used as a compliance tool – in the UK and elsewhere - once the new law is in place.

Article 6
Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83.

3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in:

(a) Union law, or
(b) the law of the Member State to which the controller is subject.
The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.

ICO comment: We have always head reservations about how well the current law's 'conditions for processing' requirement works in practice. There has always been a risk of unobjectionable, reasonable processing being prohibited for purely technical reasons. However, we recognise that this approach is very much a part of some Member States' legal systems and that there is very little chance of any change of approach within European Data Protection. It is important though that the presence – or absence – of conditions is thought through properly – particularly alternatives to consent when this is not viable.

There is a danger that processing which is necessary for public authorities but not provided for by law will be prevented. We would like to see explicit recognition that processing may take place where it is clearly in the data subject's interests and does not override his or her fundamental rights and freedoms.

As a general point, we are concerned about the number of delegated acts provided for in the Regulation, many of which deal with quite fundamental issues. This could cause a lot of uncertainty, for example here the question of what is in an organisation's legitimate interests is a very important one.

The 'legitimisation' of incompatible processing provided for in paragraph (4) will be very confusing in practice, not least for data subjects.

We are unclear that as to how Article 6 can act as gateway for legitimate processing triggered by Access to Information or Freedom of Information laws. In the UK the trigger on schedule 2 condition 6 currently offers this

gateway. We would urge consideration of an explicit article recognising the interaction with FOI/Access laws.

Article 7
Conditions for consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

ICO comment: We are in favour of a high standard of consent. We do need to be mindful of the implications of paragraph (2) though. This would mean that if consent is relied on when you buy a book online, for example, there would have to be separate consent to use your details to despatch the book and take payment. Consent could not be implied from the customer's decision to buy the book. This could be onerous and in many cases pointless. Again, in cases like this the 'legitimate interests' condition could be important as an alternative to consent.

Determining whether there is a 'significant imbalance' between an individual and a data controller is difficult to do in practice. Whilst we fully accept that genuine consent depends on freedom of choice, it is still possible to have genuine consent within a basically 'imbalanced' relationship – for example in respect of certain aspects of employer – employee data processing.

Article 8
Processing of personal data of a child

1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: There is something of a mis-match here between the UK's approach to defining a child and that envisaged by the Commission. (In the UK the concept of 'competence' is used, rather than a simple age-based system. Although of course we do have some age-based rules for example in the context of buying alcohol.) However, we would not object strongly to an age-based system in this context.

We do think, though, that a child below the age of 13 should be able to access some information society services without parental consent, for example to use a confidential anti-abuse helpline. We also believe that a child should be able to carry out simple, low-risk online activity such as subscribing to a pop-star's newsletter without adult intervention. We need to be mindful of the practical implications of this; online age verification is difficult to do without collecting a range of 'hard' identifiers that most websites would not ordinarily need to collect. We are also aware of how resourceful and determined children can be in terms of finding ways to access the content they want to see.

Article 9
Processing of special categories of personal data

1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.

ICO comment: It is not clear what "reveal" means in this context. For example, does a photograph of, say, a black person's face reveal their ethnic origin? We believe that the wording should be narrower than this so that the processing would only be caught if its purpose was to reveal,

analyse etc. a person's ethnic origin, race and the like. It is also very difficult to define political opinions, religion or beliefs.

We have always had reservations about the general concept of non-contextual sensitive data categories. However, this approach is a part of the European mainstream and is unlikely to be dropped. We do think though that sensitivity ought to reflect as far as possible the 'average citizen's' conception of what is sensitive – it is odd therefore that financial details are excluded from the definition. However, a record of trade union membership or a note in an HR file saying that an individual has been ill with a cold is sensitive.

One possibility would be for the category to be narrowed to include only genuinely sensitive personal data, such as health records, and combine this with some notion of context and risk posed to individuals.

2. Paragraph 1 shall not apply where:
(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

ICO comment: The wording "vital interests" has always been problematic. Is this only life or death, or is it protection of health or well-being more generally? A wider interpretation, going beyond life or death situations might be useful.

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or

ICO comment: We are not sure of the significance of the "profit seeking" condition here. This is a general theme that runs through the Regulation, and perhaps unfairly categorises profit-seeking activity as high risk – for example where processing done for 'gainful interest' is excluded from the personal / household exemption.

(e) the processing relates to personal data which are manifestly made public by the data subject; or

ICO comment: We need to consider whether 'made public' means published to everyone or, for example, to a large but limited number of social-networking 'friends'.

(f) processing is necessary for the establishment, exercise or defence of legal claims; or
(g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or
(h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or
(i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or
(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.

ICO comment: We are aware that some have interpreted this provision as meaning that a complete register *has* to be kept, rather than meaning that there is a restriction on who can control such a register if kept. The former interpretation is wrong, but the text should clear up any ambiguity.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.

ICO comment: Again, we have reservations about the provisions for delegated acts here. We would prefer to see these criteria, conditions and appropriate safeguards specified on the face of the Regulation to provide as much certainty as soon as possible.

Article 10
Processing not allowing identification

If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

ICO comment: We think that this is intended to deal with situations where data controllers, such as telecoms companies offering a PAYG service, do not have subscriber data but the subscriber still wishes to make a subject access request. We would like to see some clarification of what this provision is meant to do in practice.

However, it is not clear what "obliged to acquire" means. We are also unsure about the wording "do not permit the controller to identify a natural person". It is not consistent with other terminology used in the Regulation such as processing personal data about an individual. Clarity and consistency of terminology should be ensured.

We are also not sure how useful this Article is, given that if processing does not allow an individual to be identified then presumably it falls outside the scope of the Regulation anyway.

Article 11
Transparent information and communication

1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.

2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

ICO comment: We welcome clear and accessible privacy policies and this provision accords with our well-established policy approach, especially as expressed in our Privacy Notices Code of Practice.

The issue of whether privacy policies need to be merely accessible to data subjects or need to be actively communicated to them has always been a source of confusion. This is a real issue for data controllers and we would like clarification of the type of communication required. The wording of this Article as drafted does not provide clarity and perpetuates the uncertainty.

It could be disproportionate to require data controllers to actively communicate their privacy policies in all circumstances, each and every

time. However, it is our view that the transparency standard provided for here should be linked to risk. The more unexpected, contentious or objectionable the processing, the more important it is that privacy policies are communicated actively to the data subject.

Article 12
Procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

ICO comment: We think a formulation of a specified number of working days would be clearer than a calendar month. We can see why it is necessary to extend this time period where a large number of requests are made at the same time, for example as part of a campaign. "Several", however, suggests a few - that is, a fairly small number.

We do not see why a data controller who receives a subject access request electronically should be required to provide the data in a paper form, even if the data subject does request this. (Although we do not think data controllers should be allowed to provide subject access electronically in response to a request submitted 'on paper'.)

3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

ICO comment: We welcome the reference here – and others elsewhere – to the supervisory authority and judicial remedy. It is important that it is

made easier for data subjects to know where to go to pursue their issue in the event of a data controller refusing their request.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

ICO comment: If this means that subject access is now free of charge the wording should make this clearer, given the significance of this change. Our own view is that unless granting access involves a substantive administrative burden for data controllers then there should not be a fee. That said, we have no objection to a modest fee being levied in other circumstances; we receive few, if any, complaints about the current £10 fee. We do consider that there is some risk of a large volume of frivolous and/or vexatious requests if the fee is abolished. We also consider that it is necessary to include some pointers as to what is unreasonable, for example where a number of individuals act in concert with the primary intention of disrupting or inconveniencing the data controller.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.

6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: This Article indicates a recurrent theme in the Regulation, emphasis on procedures and compliance methods. We accept that policies and procedures help compliance but we are not convinced that establishment of prescriptive methods should be mandatory in all circumstances.

We dislike the use of standard official EC forms as we believe that there should be flexibility. Data controllers should be allowed to use their own judgment to decide which format is appropriate based on the format used to make the request. It is also important to understand what members of the public want here. Using a standard form and format could make

subject access information less easy to understand. Our experience suggests that there is no demand from the public for subject access information to be provided in a standardised format.

Article 13
Rights in relation to recipients

The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

ICO comment: This is welcome because it gives statutory recognition to a good-practice recommendation we made in our Data Sharing CoP, i.e. where incorrect data has been shared all the organisations which hold it should put it right. This will not always be possible to achieve in practice but is certainly an approach we support and an objective data controllers sharing data should work towards.

Article 14
Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:
(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;
(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(c) the period for which the personal data will be stored;
(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;
(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
(f) the recipients or categories of recipients of the personal data;
(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;
(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.

ICO comment: We have already set out our comments on the extent to which this information should be actively communicated as opposed to being made readily available.

We have doubts as to how useful it is to provide a citizen with the contract terms set out in (b) and it certainly seems excessive for a data controller to have to provide these as a matter of course. While we obviously support greater transparency, we wonder how much, in reality, this will empower a citizen.

We are not aware of any citizen demand for some of this information and, in fact, it could overwhelm citizens with large amounts of information. This could be counterproductive. We would prefer the emphasis to be on clear, intelligible explanations of purpose, of data controller identity and the enhanced information about sources of data and disclosures, together with the purpose for which disclosures are made. It is our view that this would provide a superior 'transparency' package for individuals which would also be less burdensome for data controllers. We would like to see some statutory recognition of the 'layered' privacy notices approach we have long supported, i.e. give people a basic notice but make a more detailed one available to those that want it. It would be very difficult to provide all the information set out above on a mobile device, for example. This is a particular issue given many individuals' apparent reluctance to read privacy notices and similar material.

The right provided for in (e) could lead to a greater number of complaints being submitted to DPAs. The resource implications of this will need thinking through. That said, it would also empower data subjects who are dissatisfied with the behaviour of a particular data controller.

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

ICO comment: Does "obligatory" mean that the individual is required by law to provide the information or that they will not receive the requested service if the information is not provided? We can certainly see the relevance of this provision though, given that it can be very unclear to individuals whether they are required to provide information or not. This should encourage good practice in terms of the use of clear 'mandatory' – 'optional' fields on data collection forms.

3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.

ICO comment: We generally like the idea of the data controller having to tell the data subject where the personal data came from – this is a valuable transparency measure – particularly in complex data sharing contexts where individuals may have little knowledge of – or control over – the sharing of their personal data. However, we do not believe that this should have to be done in each and every case. The duty should be limited to those cases where a failure to provide this information would have particular consequences for the individual, or where the source would be wholly unexpected, for example**.** Again, we would like to see an element of risk assessment introduced here. We can certainly see the desirability of individuals being informed much better about the exchange of information about them, but the practicalities need thinking through. Given the complexity of present-day information systems, as it stands this provision could result in a very large number of 'data obtained' notifications being sent to a very large number of individuals.

4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:
(a) at the time when the personal data are obtained from the data subject; or
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.

5. Paragraphs 1 to 4 shall not apply, where:
(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or
(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or
(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

ICO comment: It might be useful to extend the wording in (a) to cover those situations where the data subject already knows or might reasonably expect that to be the case. As it stands, it could be read as meaning where the data subject has already been provided with a copy of the privacy notice.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

ICO comment: It is not clear what this will entail in practice. Is it intended to mean that there should be some general 'fair processing' statement rather than actively informing individuals? This provision requires further clarification – what are the safeguards individuals can expect and what, in reality, do data controllers have to do?

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

ICO comment: It is not clear why this is necessary. Our experience of dealing with classes of recipients under our current notification system has led us to believe that this approach is of little benefit to individuals. Individuals are more concerned with knowing which actual organisations have, or are exchanging, information about them.

8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: Again, we consider that the introduction of standard EC forms is not necessary and could send out a 'bad regulation' message, depending on how these are drafted. It could also stifle innovation. Some companies, particularly those operating online, are finding innovative ways of delivering transparency. The Regulation should encourage this.

Article 15
Right of access for the data subject

1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:
(a) the purposes of the processing;

(b) the categories of personal data concerned;
(c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;
(d) the period for which the personal data will be stored;
(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;
(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
(g) communication of the personal data undergoing processing and of any available information as to their source;
(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.

ICO comment: As it is the main subject access right, we believe that (g) should be given greater prominence, that is, it should go to the top of the list and the information which has to be provided should follow it.

"Communication" requires clarification. It is not clear whether this means the data subject has the right to be provided with a copy of the data – which is what most individuals want.

We are not sure what (h) adds to explaining the purpose of the processing.

2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.

ICO comment: In our view, the right is sufficiently clear and we are not sure what a delegated act could usefully add. What criteria and requirements are envisaged here?

4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data

processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: We are unable to see why standard forms or procedures are required. The evidence we have overwhelmingly suggests that data controllers are capable of developing their own ways of verifying identity and ensuring that individuals have access to the information to which they are entitled.

The subject access request problems we encounter do not emanate from a lack of standard forms or procedures, although we accept that, in some cases, better paperwork and procedures could assist.

Article 16
Right to rectification

The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

ICO comment: Completion of "incomplete" data suggests omission or missing data. A corrective statement usually comes into play where the data is there but the data subject considers that the information is incorrect.

We are also not sure that "incomplete" data is always a problem. Data controllers will often collect only that information which they need rather than, say, completing all the fields on a form. We do not believe that this is a problem in itself, provided of course there are no adverse consequences for the individuals or other record keeping issues.

Article 17
Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Article 19;
(d) the processing of the data does not comply with this Regulation for other reasons.

ICO comment: Individuals should have stronger rights in terms of controlling the dissemination of information about them. This Article reflects a subtle but significant change to the 'balance of power' between data subjects and controllers. Currently the default position is that controllers can process personal data about someone other than in certain limited circumstances. The situation under the Regulation is that the individual has the power to prevent the processing unless the controller can justify it.

However our concern here is about how difficult (or impossible) this may be to achieve in practice and how it could lead individuals to believe falsely that they can achieve the absolute erasure of information about them. We know from the efforts of well-resourced and motivated individuals that it can in fact be impossible to remove information from the internet once it has been posted. We are concerned that this right, as billed, could mislead individuals as to the degree of protection the law can offer them in practice.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

ICO comment: Where information has been made public, i.e. has been published, it is not clear what the reasonable steps here would amount to. This provision would only work in the context of limited disclosure.

We also understand that authorisation of a third party by a data controller is unlikely. Third parties are more likely to harvest published information and republish it, often without the original data controller's knowledge let alone consent.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
(a) for exercising the right of freedom of expression in accordance with Article 80;
(b) for reasons of public interest in the area of public health in accordance with Article 81;

(c) for historical, statistical and scientific research purposes in accordance with Article 83;
(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(e) in the cases referred to in paragraph 4.

ICO comment: In (e), there may be an argument for an additional exemption from this right where the continued processing is in the data controller's legitimate interests and is not prejudicial to the interests of data subjects. This might help to deal with the situation where a customer demands that their record is erased even though the business has a legitimate reason for maintaining it, albeit that it is not legally required to do so.

4. Instead of erasure, the controller shall restrict processing of personal data where:
(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;
(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;
(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

ICO comment: We are not clear how the data controller could process the personal data anyway if the erasure has already been carried out.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;
(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;
(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Article 18
Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

ICO comment: We are aware of data controllers' concerns here surrounding intellectual property rights and trade secrets. There has also been some discussion as to whether 'data portability' should be included in data protection law as it is not a 'classical' element of it. We do not have strong views about this but welcome its inclusion in so far as it empowers citizens in consumer and possibly other contexts. It is worth noting the relevance of the UK's Midata programme here.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: There is a real danger that if the Commission specifies a format it could be one that few organisation use. It is worth remembering that many organisations use their own in-house systems to process personal data. We also need to think through the cross-European implications of this.

Article 19
Right to object

1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

ICO comment: It has always been our view that the right to object would be more helpful if it were to be framed as a 'right to prevent processing'. It is possible to object to processing without any cessation or modification of the processing actually resulting from that objection.

The data controller should be able to refuse an objection where there are compelling and legitimate grounds for it to continue processing. This would deal with those situations where individuals expect the cessation of processing in unrealistic circumstances.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

ICO comment: We consider that this could be an opportunity to tackle the issue of direct marketing objectors objecting to data controllers legitimately retaining their data on a suppression list. This provision could make it clear that this is necessary if marketing suppression is to be achieved. However, paragraph 3 below as drafted could make this impossible.

3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

Article 20
Measures based on profiling

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

ICO comment: As it stands, this provision fails to recognise that profiling takes place in very different contexts for very different purposes and with a very different effect on individuals. For example, profiling is used to subject certain individuals to additional security checks at airports as well as to direct particular online advertising to particular individuals. The degree of risk is different and this Article should reflect that. We had assumed that profiling here is meant to address online behavioural advertising; however it is not clear whether using profiling to send an ad for one product rather than another has a "legal effect" on someone or otherwise significantly affects them.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:
(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or
(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or
(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

ICO comment: Would it be acceptable if there is a mix of sensitive data with non-sensitive data? We are not sure how this provision is meant to work in practice.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

ICO comment: We consider that specification of purpose would probably suffice rather than "envisaged effects".

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

Article 21
Restrictions

1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:
(a) public security;
(b) the prevention, investigation, detection and prosecution of criminal offences;
(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;
(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d);
(f) the protection of the data subject or the rights and freedoms of others.

ICO comment: This Article would allow the UK to introduce exemptions, perhaps by retaining the ones in the current DPA, from the Regulation for crime prevention and so forth.

This Article should include the possibility of a restriction for data protection regulatory purposes, for example the detection and prosecution of data protection breaches.

Article 22
Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

ICO comment: This touches on a problem that runs through the Regulation, emphasis on compliance process rather than outcomes. Our experience of auditing companies suggests that there is not necessarily a direct link between policies and procedures and practice and, as drafted, there is a danger that companies will be led to believe that they are complying with the law because they have the required policies and measures in place. There is no doubt that organisations of any size or complexity need to have policies and procedures in place in order to deliver data protection compliance. However, that does not in itself bring

about compliance. Due weight needs to be given to outcomes for individuals and actual practice.

2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;
(b) implementing the data security requirements laid down in Article 30;
(c) performing a data protection impact assessment pursuant to Article 33;
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);
(e) designating a data protection officer pursuant to Article 35(1).

ICO comment: Rather than specify these five measures, we would prefer wording such as 'appropriate organisational measures, such as…'. We believe that there is a lack of flexibility here and we would prefer drafting that would open the way for different approaches to compliance based on the very different circumstances of very different businesses.

Clearly some of these measures will not be suitable for SMEs and we need to ensure that the derogations recognise this. Our experience suggests that a better way to encourage organisations to adopt effective compliance measures might be through guidance and/or feedback from audit activity.

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.

ICO comment: We are in favour of a verification of the effectiveness of the measures because this will encourage organisations to look at the real-world effect of what they are doing.

Clearly verification carried out by external auditors would be costly and perhaps beyond the reach of many smaller businesses. The proportionality trigger for deciding whether an external verification process is required could be difficult to apply in practice, although it is good that this does, to some extent, open the way for a more risk-based approach.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred

to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.

ICO comment: We have already expressed our reservation about the number of delegated acts, a particular problem given the significance of some of them. We are concerned here that the possible introduction of further "appropriate measures" at some point in the future could cause uncertainly for businesses and for data subjects in that they will not know what organisations are required to do to protect their personal data.

If there is to be a list of "appropriate measures" it should be finalised before the Regulation is adopted.

Article 23
Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: The ICO has very much championed privacy by design (PBD) principles and we are pleased to see them recognised in law. However, our experience of advising organisation on PBD issues has led

us to believe that the strength of the approach lies in its scalability and flexibility.

There can be no 'one size fits all' approach and there is a danger that the detailed specification of criteria and mechanisms here, effectively in a single 'rule book', could make PBD principles unattractive to (or even unachievable for) many organisations. PBD is very much a broad design philosophy and could be difficult to translate into a statutory requirement.

Article 23 (3) could be read as meaning that there will be a single set of measures, applicable across all sectors, or that there will be different ones for use in different contexts. Whilst the latter might introduce some flexibility, it would be very ambitious to attempt to provide detailed measures for use across all the different sectors.

This is why our experience of dealing with this has suggested strongly that a more 'lite', principle-based PBD approach that organisations can build upon themselves is probably the most effective way to encourage the adoption of a PBD approach.

Article 24
Joint controllers

Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

ICO comment: We like the explicit recognition that, where a number of organisations act in concert to process personal data, they need to work out what their respective responsibilities are. This reflects an approach we have promoted as good practice in our Data Sharing CoP and elsewhere.

We assume that the 'arrangement' in the latter part of this Article is meant to make it easier for individuals to exercise subject access, and other rights, in respect of shared information. This would mean, we think, that an individual could make a single SAR in order to gain access to information about him or her that has been shared between other organisations without having to make a request to each organisation. We are very much in favour of this approach.

Article 25
Representatives of controllers not established in the Union

1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.

ICO comment: It is not clear from this provision what a representative would be required to do. Is this meant to be an administrative arrangement, i.e. a point of contact between EU citizens / DPAs and non-EU data controllers? Or, is the role meant to be a more substantial one, i.e. as an entity with real assets to target if things go wrong, with funds to pay penalties and the like?

Under the current law, the representative has a very limited administrative role and our experience suggests that their role has been fairly modest in terms of usefulness to us or to citizens. However, if the representatives' role is to be expanded, then this needs to be clarified.

We also need to be realistic here in terms of the likelihood of every non-EU data controller that offers goods of services (or monitors behaviour) designating a representative in the EU, even if ones with fewer than 250 employees are excluded. There are issues as to how we could enforce this requirement. However, much here depends on what "offers goods or services" means.

2. This obligation shall not apply to:
(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41;

ICO comment: Again, this touches on the role of the representative. If the representative is meant to perform a useful function for DPAs and citizens, for example in resolving a problem they have with a non-EU organisation, then the role could be as valid in respect of an (inadequate) Colombian company as an (adequate) Argentine one.

However, we understand the thinking and the history behind this, i.e. the assumption that companies in adequate countries will not have to have representatives because they will be complying with a DP law equivalent to that in place in the EU, will therefore be subject to regulation by their own DP authorities, and will presumably not cause problems for EU citizens because of the standards of DP compliance they should have in place.

or
(b) an enterprise employing fewer than 250 persons;

ICO comment: As we have said elsewhere, this is an arbitrary threshold, not based on or related to risk of harm. 'Big' information based businesses with few employees but millions of user records could be

excluded; engineering firms with a lot of employees but relatively simple and low-risk processing operations would be caught.

or
(c) a public authority or body;

ICO comment: We need to be mindful of the difficulty of defining a public authority or body and our experience of dealing with FoI suggests this can be far from straightforward. It could be far more difficult when we need to determine whether or not an overseas organisation is a public body and a 1,000,000 EUR fine could rest on this, see Article 79 (6).

or
(d) a controller offering only occasionally goods or services to data subjects residing in the Union.

ICO comment: Again, we will find this qualification difficult to apply in practice. For example, would a camping goods store in Colorado that deals with a steady stream of UK customers be caught? Does "offering" goods mean selling them? It would be very unusual for an e-commerce site, for example, to only "occasionally" offer its goods or services. They would tend to be available all the time which, as the wording stands, could mean that virtually every non EU e-commerce site would be required to have a representative. However**,** if the company in Colorado does not deliver goods to customers in the EU then it would be difficult to argue that it is offering goods to EU citizens.

3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.

ICO comment: We think that the practicalities of this provision require further consideration. Presumably this provision means that a big electronic service provider based outside the EU but with users / subscribers across the Member States could choose to have its representative in any Member State. However, would a site that only offers its services in say English be said to be offering its goods and services to Latvian speakers?

This could be argued either way but, given the relative dominance of English in e-commerce and electronic service delivery more widely, this could have a greater effect on the UK (and therefore the ICO) than on other Member States.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

ICO comment: This suggests action could be taken against either the controller or the representative, which begs the question once more of what the role of the representative actually is.

Article 26
Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.

2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

ICO comment: It is fair to say that the ICO can find it difficult to determine which organisations are data controllers and which are processors. The problem arises because, given the collaborative nature of modern business, it is rare for a one organisation (the processor) to only act on instructions from another (the controller). There tends to be a considerable degree of freedom, skill, judgment and the like in terms of the way the first organisation provides services to the second, all against the backdrop of complex collaborative arrangements involving numerous organisations.

In short, we need to be clear about who is responsible for what where a number of organisations are each involved in the processing of personal data, and, as drafted, this Article will not help us here.

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30;

(d) enlist another processor only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

ICO comment: There is perhaps some contradiction between the inert role of the processor and the obligation on it here to comply directly with DPA requests. However, we could find this duty useful in our investigative work.

3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.

4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.

ICO comment: We can certainly see why a processor that takes a controller's data and then uses it for its own purposes should take on full data controller responsibility.

However, this is different from failing to act on the data controller's instructions. We would have more difficulty with the idea that a processor becomes a controller because it has erased personal data by mistake, for example – this would amount to processing personal data other than as instructed by the data controller -but in a case like this the organisation should just be treated as a 'bad processor' rather than a data controller in its own right.

Article 28
Documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

ICO comment: Again, we believe that there may be too much emphasis here on the compliance paperwork. If this is intended to be of use to DPAs when carrying out their enforcement work, our experience would suggest that, even though an organisation may be able to produce the 'paperwork', its actual procedures may fall short. We have no problem, though, with a data processor adopting good information handling practices such as knowing which data processing activities it is carrying out for which data controllers.

This provision could impact significantly on SMEs.

2. The documentation shall contain at least the following information:
(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
(b) the name and contact details of the data protection officer, if any;
(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
(d) a description of categories of data subjects and of the categories of personal data relating to them;
(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
(g) a general indication of the time limits for erasure of the different categories of data;
(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

ICO comment: This documentation will be kept and made available on request to the ICO. We can see the advantages of larger organisations developing their own systems and procedures for ensuring DP compliance. However, it seems that this documentation is intended to assist the supervisory authority (i.e. the ICO) in carrying out its compliance activities. As we have explained elsewhere, there is a danger that companies will focus on the 'paperwork' rather than on actual data protection compliance. As such, organisations with good practices but

'poor paperwork' will be at a disadvantage to those with bad practices but 'good paperwork'. Our experience of carrying out audit of organisations suggests this could be a real risk. (The risk would be compounded if a 'paperwork' check were to take place without any examination of actual practices.)

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:
(a) a natural person processing personal data without a commercial interest; or
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

ICO comment: The "commercial interest" formulation is problematic here. There is no obvious reason why a natural person processing personal data in pursuit of a commercial interest presents a greater risk than one doing so for non-commercial reasons.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 29
Co-operation with the supervisory authority

1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.

2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.

Article 30
Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

ICO comment: We welcome the extension of "appropriate measures" to processors and the flexibility of the wording. This appears to allow for the scalability that the current law provides for.

However, paragraph 3 below, suggests that there could be a detailed 'rulebook' for technical and organisational security, such as those that some DPA's already produce, which could undermine this flexibility.

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.

ICO comment: We dislike the inclusion of the wording "state of the art". We tend to consider accepted industry standards when breaches arise from technical failings such as hacking, rather than whether security measures were "state of the art".

There is a real danger that detailed, specific security criteria will soon be out of date, for example those relating to encryption strength. Our experience suggests that one of the widely acknowledged strengths of the current law is its technological neutrality, especially in the security sphere. This must not be jeopardised.

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:
(a) prevent any unauthorised access to personal data;

(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;
(c) ensure the verification of the lawfulness of processing operations.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: We have some doubt as to how an "implementing act" might be used to deliver compliance in respect of some of these matters. How, for example, might a legal text be framed that would prevent the unauthorised reading of personal data?

Article 31
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.

ICO comment: We have explained that the timescale here is unrealistic and that, while a well-designed data breach notification process could serve the public well, we need to get the 'triggers' right. This seems to be one of the features of the Regulation that has received a lot of negative press. There may also be a case for notifying data subjects at the same time as, or conceivably before, the supervisory authority is notified.

Again, we would like to see an element of risk introduced here, as clearly some breaches will be more consequential than others.

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.

ICO comment: We need to be careful about what "immediately" means but we do support the duty for processors to inform controllers of a breach as a matter of urgency.

3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;
(d) describe the consequences of the personal data breach;
(e) describe the measures proposed or taken by the controller to address the personal data breach.

ICO comment: We need to ensure consistency here with the current breach notification rules under PECR (UK implementation of the EU's ePrivacy Directive), otherwise many data controllers will need to operate under two different regimes. This needs to be harmonised, especially given that PECR is no longer a 'niche' piece of legislation. Please note that PECR requires breach notification 'without undue delay', it does not specify a timescale.

We should be mindful of the recent Art 29 WP paper that supports a 'two step' notification scheme. This recommends an initial notification within 24 hours, followed by a more detailed notification 3 days later. We nevertheless have some reservations as to how useful this 24 hour notification requirement would be in practice and have concerns that a two–step notification scheme could cause complications and add complexity. Although a two-step system is not provided for in the Regulation, given the influence of Art 29 'opinions', this may well surface as a proposed amendment.

We have doubts as to whether 3 days will necessarily be long enough for companies, for example large electronic service providers, to conduct and complete an investigation into a breach. It could also be confusing for companies to be expected to comply with two different notification deadlines.

Whilst we recognise the benefits of breach notification, we have concerns that a dual notification requirement will result in increased bureaucracy for both organisations and the ICO, with little benefit in terms of strengthening data protection for individuals. We also need to be mindful of the logistical implications for ICO of having to deal with a possibly very large number of breach notifications, some of which may be relatively trivial or insignificant.

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.

ICO comment: It is not clear what this documentation would be used for in practice or how the supervisory authority would gain access to it. If this documentation is meant to be produced within the '24 hour' rule, it could

be difficult for controllers to assess the effects of a breach or to take any remedial action before filing its report.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.

6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: We reiterate our remarks about the need to consider breach notification in the context of the e-Privacy Directive (PECR). However it is important that we learn from our experience of applying the breach notification requirements in the E-privacy Directive (PECR) and do not simply replicate its provisions. It is important that, as far as possible, we have a coherent approach and avoid a dual notification system resulting from two separate pieces of legislation. This need for coherence also applies to the use of delegated acts.

Article 32
Communication of a personal data breach to the data subject

1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

ICO comment: We are in favour of this, provided that we can get the triggers right. In this case that depends on what an "adverse effect" is. We cannot see why the Article 31 communication (i.e. to the supervisory authority) should always happen before the Article 32 communication. This should depend on the circumstances and, in some cases, there could be a case for informing data subjects immediately or without undue delay (note the inconsistency of wording here) and before the supervisory authority is informed, for example where an individual is left open to the risk of identity theft or financial loss.

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the

information and the recommendations provided for in points (b) and (c) of Article 31(3).

3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

ICO comment: We do not wish to re-open the 'personal data' issue here but we would take the view that, where encrypted data is lost but the decryption key remains safe, there will not have been a "personal data breach". However, it is welcome that the duty to notify the data subject does not apply where only encrypted data is lost. (This begs the question, though, of why such a breach need be notified to the supervisory authority.)

4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.

ICO comment: This should presumably say "adversely affect the" 'data subject'. Again, we reiterate our general belief that criteria like this need to be specified on the face of the Regulation itself, otherwise there could be a long period of uncertainty for data subjects and organisations regarding the circumstances in which a data subject needs to be informed of a breach. It is likely that the ICO will need to produce guidance as soon as the provisions come into effect but this could then be superseded by a delegated act – leading to uncertainty and confusion for data controllers.

Article 33
Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf

shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

ICO comment: The ICO has been very supportive of Privacy Impact Assessments and is pleased to see an equivalent measure provided for in the Regulation. However, we do need to get the 'threshold' right for carrying out a DPIA and we would like to see some flexibility in terms of what a DPIA involves. As with other features of the Regulation we fear that a single 'approved' DPIA methodology might make the valuable DPIA process inflexible and unattractive to some data controllers, especially SMEs.

The term "envisaged" presumably means that the DPIA will only apply to 'future' processing operations. There may be a case for carrying out a DPIA on an existing process operation where this is high risk and has not been done already. We know that some organisations carry out PIAs periodically and this can serve as a useful privacy review process.

2. The following processing operations in particular present specific risks referred to in paragraph 1:
(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;
(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
(d) personal data in large scale filing systems on children, genetic data or biometric data;
(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).

ICO comment: While the criteria stipulated here are along the right lines, the detail of this paragraph needs further thought. In our view, there should be greater focus on large scale, systematic, high profile and high volume processing. Some of these criteria, for example the evaluation of personal aspects relating to a natural person, could be very difficult to apply in practice and could make the circumstances in which a DPIA is required very wide.

The ICO's PIA Handbook explains more about the threshold for carrying out a PIA.

3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

ICO comment: We welcome the involvement of the public here but this is only really essential where a novel, large-scale and potentially privacy-invasive processing operation is envisaged. An obvious example would be the use of citizens' panels or focus groups where a new government database or service is being planned. Ideally, there should be a requirement to take the public's views into account, although this is probably implicit in this provision.

5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.

ICO comment: It is helpful that particular reference is made to consideration of specific measures for SMEs.

However, provision for a delegated act means that there is a significant risk of a weighty piece of additional legislation setting out the PIA criteria. Our experience of helping organisations to carry out PIAs, and of carrying out our own PIAs, suggests that there needs to be considerable flexibility in terms of the scale, methodology, thresholds and the like for carrying out a PIA.

7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: It is not clear who will carry out the verification and auditing here; does this mean the organisation carrying out the DPIA? As far as we are aware it is unusual for an organisation to audit its own 'compliance' with a DPIA. Normally it would use a DPIA to assess the privacy impact of an envisaged data processing operation and then to either go ahead, go ahead with modifications or not go ahead.

It is not clear what the role of the DPA is here, if any. However, we would prefer it if the supervisory authority or the EDPB were to issue guidance relating to how DPIAs should be carried out.

Article 34
Prior authorisation and prior consultation

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.

ICO comment: The concept of prior authorisation is wholly new for some supervisory authorities, such as the ICO. We are not aware that our current approach to regulation in this area has resulted in any failure to protect personal information.

It is not clear when the controller or when the processor will be required to obtain an authorisation.

It our understanding that the provision for prior authorisation will apply where a controller or processor adopts a non-standard data protection clause or non-BCR basis for making a transfer. This could have a significant impact on us as a regulatory body if we were required to authorise these in advance. The sheer scale of this duty must not be underestimated.

As with all prior-checking and authorisation, there is a risk that a data processing operation, which may well be for the public good and carry

negligible privacy risk, would have to be 'put on hold' whilst the authorisation process takes place. Given the comment above about the logistical implications, a backlog of cases could build up very quickly.

2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:
(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or
(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.

3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.

ICO comment: It is confusing to refer to special categories of data in the Regulation but to then refer to categories "likely to present a high degree of specific risks" to be maintained in the list. (Although the list will be useful in terms of drawing data controllers' attention towards high-risk processing operations.) If we are to have 'special' and 'ordinary' processing operations then we need a clear and consistent formulation and need to decide whether this is based on data classes (special / non-special) or on risk posed by the overall processing operation, as seems to be envisaged here, and the latter is an approach we prefer.

5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.

ICO comment: This is presumably meant to ensure that where a data controller is operating across Europe, all the DPAs will be in agreement as

to whether its processing operation appears on the 'list'. Whilst we can see the benefits of a consistent regulatory approach, it is still not clear to us what the practical effect of the list will be, for example to individuals.

6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

ICO comment: This Article appears to stipulate that if a DPIA indicates that processing is high-risk, the data controller must submit it to the DPA. However, even where the DPIA does not indicate a high risk, it must still be submitted to the DPA, albeit that we do not need to authorise it. That poses the question as to what it is we are required to do with such information. Is every Article 33 DPIA to be submitted to us?

Is this Article intended to mean that we, as supervisory authority, see the DPIA regardless, or is it intended to mean that we only obtain the DPIA either where the processing is deemed to be high risk or where we ask to see it? As currently drafted, our supervisory role here could be extremely wide and would encompass supervision of non – risky processing.

7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

ICO comment: We are all for legislators seeking the views of the DPA when it is planning new law that will involve the significant processing of personal data. For example we often work with bodies like the Home Office in situations like this. We hope that this will continue.

However, we are not sure how this provision is meant to work. Does law that "defines the nature of the processing" mean law that specifically addresses the scope of data protection law? Presumably not as the Regulation itself will do this. Or, does it mean that the Member State, i.e. the government, has to consult the DPA in respect of any law that merely *involves* the processing of personal data. As law is generally meant to allow individuals to do things or to stop them doing things, then this could mean that virtually all law has to be consulted on.

The logistics of this require further consideration. At some times in the Parliamentary calendar a great deal of legislation is being introduced,

most of which will probably provide for the processing of personal data to some extent. If a consultation process is to be meaningful, this could cause considerable delay in the legislative process and the DPA could well be overwhelmed with requests for consultation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 35
Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
(a) the processing is carried out by a public authority or body; or
(b) the processing is carried out by an enterprise employing 250 persons or more; or
(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

ICO comment: We know from our experience of FoI that it is not always clear whether an organisation is a "public authority" and the same problems of scope could arise here.

It would be better if it could be made clear that there needs to be someone with data protection responsibility – this need not necessarily be a particular officer.

We can see it proving difficult to determine which processing falls within (c) and this is yet another variant of the Regulation's formulation for determining risk. As stated above, there needs to be a clear and consistent approach to defining the riskier forms of processing.

A simple head-count criterion for the designation of a data protection officer is not the best approach. It fails to recognise that some low head-count companies process a large amount of often sensitive information about a lot of people – social networking sites for example. On the other

hand, large head-count companies – car manufacturers for example, may carry out relatively small-scale, low-risk processing.

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.

ICO comment: Some public authorities, for example a local group of parish councils, should be able to do this too.

3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.

ICO comment: It is not entirely clear what an "entity" is in this context. Presumably it might mean the various regional offices of a government department, for example.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.

ICO comment: This could devalue the worth of DP Officers. Does this mean, for example, that an engineering trade body could appoint a single DP Officer for all engineering firms with fewer than 250 employees? Whilst we are all for removing unnecessary burdens, this could make the role of the DP Officer 'symbolic' and ineffective in practice.

5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.

ICO comment: This seems to mean that the DPA may be required to assess the expert knowledge, practices and ability of the DP Officer. How are we to do this? Whilst we have an ISEB DP qualification here in the UK, we are not aware of such a qualification in other Member States. Of course we cannot assume that having this qualification means that the standards required by the Regulation will have been met.

This provision is also rather prescriptive in terms of who an employer can hire. A better suggestion may be to have sufficiently robust knowledge, practices and procedures in place within the group or within a company, as DP compliance tasks are often shared between departments and staff members.

It could be problematic for a DP Officer to be afforded such a special and unusual level of employment protection. It is not clear what the consequences of dismissal of a DP Officer in such circumstances would be.

A data processor should not be required to appoint a DP Officer.

6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.

7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.

ICO comment: If a DP Officer were to be dismissed, to whom would he/she complain? Presumably, in the circumstances set out, the employer would be breaching the Regulation, suggesting that the DPA should have some involvement. This could clearly be highly problematic and could lead DPA's into the realms of employment law.

We do not think the Regulation should specify employment contract terms. We question why a DP Officer must be appointed for at least 2 years by a company that generally, and quite lawfully, uses shorter fixed-term or temporary contracts.

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

ICO comment: It seems inconsistent that a service contract can be used but, if actually employed as a staff-member, the DP Officer has to be appointed for at least 2 years.

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.

ICO comment: This provision would be more effective if, instead of having the right to contact the DP Officer (something a member of the public could do anyway), it required the DP Officer to hear individuals'

complaints and ensure any necessary remedial action where there has been a problem, for example.

11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.

ICO comment: This is moving inappropriately close to providing a 'person specification' for the role.

Article 36
Position of the data protection officer

officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

ICO comment: This could be unrealistic in terms of a failure to appreciate the extent to which the processing of personal data does, to some degree or other, underpin most normal day to day business activity. It could be impossible to carry out the role as stipulated here in a company of any data processing complexity.

2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

ICO comment: The "does not receive any instructions" formulation is obviously problematic. It would be perfectly feasible for a DP Officer to act independently whilst complying with a company code of conduct or reasonable managerial instruction, for example.

3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Article 37
Tasks of the data protection officer

1. The controller or the processor shall entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;
(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;
(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;
(d) to ensure that the documentation referred to in Article 28 is maintained;
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;
(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;
(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;
(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.

ICO comment: This would convert into a rather challenging job description – which suggests again that the Regulation should open the way for a corporate approach as an alternative to the appointment a particular individual. This would reflect the way many larger organisations approach compliance in this area.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.

Article 38
Codes of conduct

1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:
(a) fair and transparent data processing;
(b) the collection of data;

(c) the information of the public and of data subjects;
(d) requests of data subjects in exercise of their rights;
(e) information and protection of children;
(f) transfer of data to third countries or international organisations;
(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;
(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.

ICO comment: The wording of this provision suggests that DPAs cannot draw up codes themselves but merely encourage others to do so.

2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.

ICO comment: The wording that the draft code of conduct or the amendment "is in compliance with this Regulation" is problematic. It is the processing that the code relates to which must be done in compliance with the Regulation, not the code itself. 'Furthers compliance with the regulation' would be a better formulation.

In addition, we are of the view that the data controller should seek the views of data subjects, not just the DPA.

3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.

ICO comment: It would be more appropriate for these to be submitted to the EDPB or even a 'lead' DPA, rather than to the Commission.

4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

ICO comment: DPAs should have a clearer role in authorising other bodies' codes of conduct at a national level. Again, we question the appropriateness of the Commission's involvement here, it would be better if this duty fell to the EDPB.

Article 39
Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

ICO comment: We are very much in favour of this provision. We welcome the flexibility it contains and its recognition that different types of activity will need different types of scheme. Our experience suggests that a scheme that seeks to address every aspect of data protection compliance will fail. Schemes need to be selective in their coverage and, in a consumer context for example, may need to focus on information collection / use and security and the like, and not attempt to cover international transfers, privacy by design, the appointment of DPO's and all the other features of the legislation. Recognition of the development of privacy seals etc. by sector based trade bodies, for example, would be useful.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

ICO comment: A clearer role for DPAs and possibly the EDPB should be set out here.

3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals

and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

ICO comment: We are not convinced that this is a matter of "technical standards". There should be a clearer role for the DPAs in terms of the on-going maintenance and audit of these schemes.

Article 40
General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

ICO comment: This is a more flexible and realistic approach that that set out under the current Data Protection Directive. However, we have reservations about an authorisation process in general and we do not believe that it is the most effective way of protecting rights.

The vast majority of cases will require authorisation unless there is/are:

- adequacy
- approval of BCR – by the ICO in conjunction with the consistency mechanism
- standard model clauses which will continue to exist – see Article 41(8) – which is welcome, and
- standard DPA clauses with EC approval.

That said, all of the above methods will still require prior authorisation by the supervisory authorities in some form, i.e. of the template clauses or of the draft BCR – apart from there an EC-approved model clause is in place. These approvals are not of individual transfers but of the mechanism by which a transfer can be made. By way of example, the concept of approving a BCR does not cover individual transfers as the approval is of a set of rules by which all entities within a multinational group are bound.

As these methods will not be suitable in a lot of cases, specific prior authorisation by the DPA of the individual transfers would be needed, for example, where ad hoc clauses are being used or there is no legally binding instrument to ensure the protection of the rights of the individual.

This requirement to authorise transfers is very different from the current UK approach as the ICO has always taken the view that the responsibility for ensuring that international transfers are made in accordance with the law rests with the data controller making the transfer. The prior approval by a DPA does not necessarily provide more protection to the data subjects in an increasingly online world and it is difficult to see how it will be possible for all relevant transfers to receive a prior authorisation.

The introduction of prior authorisations for transfers would be a large burden on the ICO as we do not currently issue such authorisations and would be starting from scratch in relation to all transfers, in contrast to other DPAs.

Article 41
Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation in question has entered into.

ICO comment: The criteria above do not fit with assessing adequacy on a sectoral basis. This also allows no room for discretion as it will be for the Commission to decide and assess 'adequacy'.

The EDPB could play a greater role in advising the EC.

3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

ICO comment: The idea of allowing data to be transferred to a "processing sector" is a good, pragmatic one and could open the way for legitimate transfers to a 'safe' sector within an 'unsafe' territory. This would be a useful option in many cases.

4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).

ICO comment: We believe that an 'inadequacy' list would be fraught with political difficulty. The idea that data cannot be transferred to certain countries is highly problematic and logically unnecessary given that the countries that data can be legitimately transferred to are already known. Although it is currently possible to deem a country 'inadequate', this has never been done and there are good reasons for this.

6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.

ICO comment: It is not clear from the wording of this provision whether the decision to prohibit transfers "without prejudice to Articles 42 to 44" means that transfers could continue as long as they are made under those provisions or whether any previous transfers made under those Articles would now be declared unlawful.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.

8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.

Article 42
Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
(a) binding corporate rules in accordance with Article 43; or
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to

processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

ICO comment: Article 42(1) appears to contradict Article 42(5) as it states that personal data can only be transferred if appropriate safeguards have been adduced in a legally binding instrument. Article 42(5) envisages, however, that transfers could be made without a legally binding instrument provided there is prior authorisation from the supervisory authority.

There is a lack of information about what would amount to "appropriate safeguards… not provided for in a legally binding instrument". Would it include, for example, a CoP? The recitals seem to suggest this.

This requirement to obtain authorisation from the ICO could cause difficulties in terms of timescales and its impact on industry. With regard to resources for the DPA, it currently takes 9 months to 1 year from receipt of the first draft of the BCR to it being approved by the relevant Authorities. (There are 36 approved BCRs across all DPAs and the UK has been lead authority on 15 of these applications.)

Article 43
Transfers by way of binding corporate rules

ICO comment*:* On a general point, BCRs only provide a mechanism to enable transfers within a multinational group and so may not be appropriate for many transfers i.e. between different companies. We are also aware that several Member States currently do not accept the validity of BCRs as a mechanism for enabling international transfers, but their positions will presumably change as a result of the introduction of the Regulation with its specific reference to BCRs.

1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:
(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;

ICO comment*:* We suggest that reference should be made in this paragraph to every 'relevant' member as not every group entity will necessarily be covered by BCRs, as it is for the company to determine which of its entities will be subject to the BCRs.

(b) expressly confer enforceable rights on data subjects;
(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules shall at least specify:
(a) the structure and contact details of the group of undertakings and its members;
(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
(c) their legally binding nature, both internally and externally;
(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;
(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;

ICO comment*:* This provision differs from the position under the current EU controller / processor standard contractual clauses 2010 and the Article 29 Working Party Paper (WP195) in relation to Processor BCR, as a processor can be based outside the EEA and is not required to have an entity established in a Member State.

Is it now intended that there should be an entity in one of the Member States? If so, the current criteria for Processor BCR will be affected and it would not be possible to approve a BCR where there is no EU entity.

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;
(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;
(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;
(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;
(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

ICO comment*:* There are many variants in the concept of what is 'legally binding' across the various Member States. Whilst the Commission will be empowered to specify other criteria, it will not do so in relation to the concept of 'bindingness' (at Article 43(2)(c)), which is one of the major issues in considering a BCR application and a current topic of much debate amongst the DPAs.

Article 44
Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

ICO comment: We welcome an approach whereby a data exporter has to consider alternative mechanisms for transfer before seeking derogation. It could be stated more clearly that derogation should only be used where an alternative mechanism has been considered but is not possible.

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or
(d) the transfer is necessary for important grounds of public interest; or
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or
(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

ICO comment: There is no detail explaining what is meant by "frequent or massive". Is this to be determined on a cumulative basis per data controller or processor, or all transfers to a particular recipient, or all transfers no matter the specific destination?

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation

by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.

4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.
5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.

6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Article 46
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.

2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

ICO comment: Overall Chapter VI is very prescriptive about the roles of DPAs and we believe many of these articles could be merged into a broader framework, containing a set of principles member states should follow when legislating to set up DPAs and resourcing them etc.

Article 47
Independence

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

ICO comment: We gather that the reference to 'members' is meant to mean the heads of a DPA – thus in the UK the 'member' would be the Information Commissioner. So, we assume that references to 'members' would in reality mean the DPA corporately.
Following "neither seek nor take instructions from anybody" it would be useful to add a qualification that focuses on the discharge of DPAs' functions. DPAs are clearly not above the law - the focus needs to be on the independence of regulatory activity.

Article 48
General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.

ICO comment: The 'new blood' introduced by Commissioners from non-DP backgrounds can be very healthy and the Regulation should allow for this possibility.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.

4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.

Article 50
Professional secrecy

The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

ICO comment: This suggests that "members" are different from "staff" – clarification of this would be useful. As with the current Data Protection Act's section 59, this provision may sit uncomfortably with the transparency agenda. This has caused us problems in terms of publicising our enforcement activity, for example. It would be helpful if there was an additional provision was added, recognising the importance of transparency and the need to balance this with secrecy.

Article 51
Competence

1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.

2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.

3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.

ICO comment: We can certainly see the advantages in a 'lead data protection authority' approach. However, we need to be clear as to whether the "main establishment" criterion is meant to be an objective

test or to allow organisations to 'choose their DPA'? Our preferred approach would be for the DPA's (possibly with some form of oversight from EDPB) to choose who regulates a particular data controller, rather than the data controller doing this. This is important given the possibility of 'forum shopping'. However, we recognise that the Regulation's consistency mechanisms should, in theory, reduce the attractiveness for data controllers of being regulated by one DPA rather than another.

We need to consider how data controllers which do not have a main establishment or a representative in the EU are to be dealt with. The simple answer is that no DPA would need to deal with them, yet, if such a company offers goods or services to EU consumers, then the Regulation is meant to apply to them.

Article 52
Duties

1. The supervisory authority shall:
(a) monitor and ensure the application of this Regulation;
(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

ICO comment: DPAs' complaint handling function is important. We have never been keen on our current duty to assess a data controller's compliance with the DPA. The public want their issues to be resolved, rather than a determination as to whether the law is being complied with – the wording should reflect this. It is also important that DPAs enjoy a reasonable degree of discretion in terms of deciding whether to take on a particular complaint and how to deal with the ones they do take on.

(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;
(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;
(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

ICO comment: It would be useful to clarify whether (f) applies to measures specifically to do with data protection or whether it could extend to any law that involves the processing of personal data, for example new criminal justice provisions. (Most law involves the collection and use of information about individuals to some extent.) The "shall… be consulted" construction suggests this places a legal duty on our institutions to consult the DPA. The constitutional implications of this need thinking through.

(g) authorise and be consulted on the processing operations referred to in Article 34;
(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);
(i) approve binding corporate rules pursuant to Article 43;
(j) participate in the activities of the European Data Protection Board.

2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention.

ICO comment: This provision is welcome. There has been a tendency for some DPAs to drop their promotional and educational work in favour of greater enforcement activity. We think this is a mistake and we are pleased that DPAs will be required to deliver a mix of activities, including promotion and education.

3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.

ICO comment: We also welcome the requirement for DPAs to provide advice to the public.

4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.

5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.

6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

ICO comment: It is certainly important that DPAs should be able to reject manifestly excessive requests. However, they should also enjoy the discretion to reject complaints which are trivial, vexatious or which lack merit.

Article 53

Powers
1. Each supervisory authority shall have the power:
(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;
(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;
(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;
(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;
(e) to warn or admonish the controller or the processor;
(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;
(g) to impose a temporary or definitive ban on processing;
(h) to suspend data flows to a recipient in a third country or to an international organisation;
(i) to issue opinions on any issue related to the protection of personal data;
(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.
2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:
(a) access to all personal data and to all information necessary for the performance of its duties;
(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried

out there. The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.
3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).
4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

ICO comment: We are content with the range of powers provided here but clarification about whether this is an exhaustive list will be important. The list does not include any mention of audit/inspection powers, which are different to investigatory powers. It is also important (linked to Article 78) that Member States are not precluded from giving DPAs powers related to criminal prosecutions, including search warrants.

Article 56
Joint operations of supervisory authorities

1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.

2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay.

3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory

authority's national law. The host supervisory authority shall assume responsibility for their actions.

ICO comment: This provision, and the general approach in the Regulation, raises a number of issues regarding different criminal offences, evidence requirements and judicial procedures in the different Member States. This perhaps assumes a degree of harmonisation of our legal systems that we have not achieved.

Article 57
Consistency mechanism

For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.

ICO comment: It would be better to involve the EDPB rather than the Commission here.

Article 58
Opinion by the European Data Protection Board

1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.

2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:
(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or
(b) may substantially affect the free movement of personal data within the Union; or
(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or
(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or
(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or
(f) aims to approve binding corporate rules within the meaning of Article 43.

ICO comment: This duty could be very wide and onerous. For example, our dealing with a complaint about any sizeable e-commerce company could fall within (a). Some of these criteria, for example those set out in paragraph (b), could be very difficult to assess in practice and could be

highly subjective. There is a danger that DPAs' ability to deal with the public's complaints etc. could be hampered unnecessarily by the need to inform EDPB / the Commission of its measure. We can certainly see though why this could be useful where a significant pan-European issue is being dealt with. DPAs must be able to exercise discretion and use their experience to identify cases where EDPB / the Commission needs to be informed. (We have some reservations about the involvement of the Commission here.)

Article 60
Suspension of a draft measure

1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:
(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or
(b) adopt a measure pursuant to point (a) of Article 62(1).

ICO comment: Essentially this means that both the EDPB and the DPAs can be overruled by the Commission - this could raise issues as to the independence of our data protection institutions.

Article 63
Enforcement

1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.

ICO comment: We need to think through the implications of this degree of harmonisation. It could lead to the prohibition of a processing operation which is acceptable to the citizens of the UK – or – on the other hand – to unacceptable processing being legitimised on the basis of a simple majority vote.

Article 65
Independence

1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.

ICO comment: This provision sits uncomfortably with Article 64(4) (the Commission's right to participate in EDPB activities etc.) and the presence of Commission staff at EDPB meetings, for example.

2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

ICO comment: If the Commission overrules an EDPB decision, as it can under the Regulation, then is it not the case that the EDPB will be required to "take instructions" from it, in contravention of this provision? In our opinion this goes against the spirit of DPAs' independence.

Article 69
Chair

1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.

ICO comment: We are not clear how this can provide for an election if one of the deputy chairpersons has to be the EDPS.

Article 72
Confidentiality

1. The discussions of the European Data Protection Board shall be confidential.

ICO comment: We can appreciate the need for confidentiality in some circumstances but transparency, rather than secrecy, should be the basic default position. We are conscious of the tension that could arise between the need for DPAs and EDPB to be transparent and publicise their work yet create 'space' for confidential policy development and relations with data controllers and others. We are aware of criticism of the current Art. 29 Working Party's on grounds of its lack of transparency and unwillingness to consult with data controllers and others. We would like to see this rectified in the future. Building an aspect of greater transparency through interaction with the outside world can improve the effectiveness of the EDPB's opinions and measures.

2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with

Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.

ICO comment: Member States' FoI laws should be taken into account here. We would reject the approach of *all* documents being submitted to EDPB *always* remaining confidential.

Article 73
Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.

ICO comment: We are not satisfied that there is a 'consumer' demand for this and, even if there were, there could be other more informal, 'lighter' ways of achieving the same outcome through DPA liaison work. Therefore, we consider that this provision is perhaps somewhat idealistic and does not reflect data subjects' expectations here.

How this would operate in practice is less than clear. It is our view that a data subject should approach their own DPA in the first instance, or the DPA in the member state where the controller is established. There are a number of logistical difficulties with this provision which require further thought and as it stands it could mean that a citizen in Finland could complain to the UK's DPA about a Greek data controller. Whilst it is unlikely that many data subjects would want to do this, the wording as it stands would allow this.

2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data.

ICO comment: This provision gives welcome statutory recognition to civil society organisations' ability to submit complaints to DPAs, although it is not clear what "properly constituted" means here. Nor is it clear whether data subjects have to give their consent before a third party can act on their behalf. If a third party is to act on a data subject's behalf, the data subject should have agreed to this.

Article 74
Right to a judicial remedy against a supervisory authority

1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.

2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State.

ICO comment: The concept of DPAs taking legal action against one another is problematic and it is not at all clear how this provision fits with the consistency mechanism. What if the data subject is resident outside the EU? Again, we wonder how much demand there will be for this facility in practice. For our own part, we are not aware of anyone complaining to us about the decision of another DPA.

Article 75
Right to a judicial remedy against a controller or processor

1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers.

ICO comment: The jurisdictional issues here seem to be a little confusing: a data subject can complain about a data controller to any supervisory authority but must either bring proceedings in the courts of

the MS where the DC or data processor is established or where the DS is resident. There is an inconsistency here.

3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.

ICO comment: This envisages communication between the courts or the courts and the supervisory authorities. We are not clear as to how this would be done in practice. However, we do welcome the recognition of an existing principle.

4. The Member States shall enforce final decisions by the courts referred to in this Article.

ICO comment: What does "Member State" mean here, the courts, the government or the supervisory authority?

Article 78
Penalties

1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.

ICO comment: We understand that the Regulation does not (and cannot) prescribe any criminal penalties. Therefore our own DPA offences, where not covered by the Regulation and where not incompatible with it, would presumably still exist on our statute book. However, we would welcome clarity on this point from the Commission and / or the MoJ. It would be a retrograde step if we were to lose our existing criminal offences.

We presume that Article 78 would therefore operate to allow us to criminalise some of the activities covered under the Regulation.

2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.

ICO comment: We understand that this provision could allow both parties to be fined. See our comments elsewhere about the role and liability of representatives.

Article 79
Administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.

ICO comment: These are reasonable criteria and – in short – allow bigger fines for more serious breaches, rather than minor technical infringements. We welcome the approach of setting out all the possible breaches in one place on the face of the legislation. This is transparent and makes it clear up front what a data controller is required to do. However, rather than having different sets of more and less serious breaches – linked to fine levels – we would prefer a single non-ranked list of breaches. An additional clause should allow for the seriousness of the breach – whatever the breach is – to be taken into account when determining the penalty. This would be a more realistic and flexible approach and would allow all the circumstances surrounding a particular breach to be taken into account. In some cases, for example, a failure to apportion responsibilities between data controllers could have more serious consequences than a failure to comply with a data subject objection. Our suggested approach would deal with situations like this and would offer the best protection to individuals by allowing DPAs to levy greater fines where there has been greater damage.

3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:

(a) a natural person is processing personal data without a commercial interest; or
(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.

ICO comment: We do not think the possibility of a warning should be linked solely to enterprise size or type. It should be linked to the seriousness of the breach and its effect on individuals.

4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

ICO comment: "intentionally" is very difficult to prove evidentially. The term requires further explanation and qualification. In many cases negligently or recklessly will be the most important trigger.

There are problems regarding the link between fine levels and turnover – how would this apply to a local authority, for example? There could be significant accountancy problems here.

We also need to think through issues regarding non-Euro states and the relative value of the Euro in the various Member States.

(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);
(b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).

5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:
(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;
(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;
(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;
(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;
(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;
(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);

(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.

6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:

(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;
(b) processes special categories of data in violation of Articles 9 and 81;
(c) does not comply with an objection or the requirement pursuant to Article 19;
(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;
(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;
(f) does not designate a representative pursuant to Article 25;
(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;
(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;
(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;
(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;
(k) misuses a data protection seal or mark in the meaning of Article 39;
(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;
(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);
(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);
(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.

ICO comment: As we have explained above, we like a clear, transparent list of the various breaches but a more flexible approach based on a single non-ranked list, with the actual effect of the breach being taken into account, would provide better protection to individuals.

Article 80
Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

ICO comment: We welcome the need to balance privacy rights with the need for freedom of expression in journalistic and other contexts. This is likely to prove one of the most contentious areas in the next phase of data protection law, especially as the concept of journalism has evolved well-beyond its traditional boundaries. We are not able to comment substantively on this Article at this time. We are awaiting the outcome of the Leveson inquiry, as clearly this will have a fundamental impact on the UK's approach here.

Article 81
Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:
(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another

person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or
(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or
(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

ICO comment: There has been some criticism that this expanded version of 'medical purposes' will undermine patient confidentiality and allow health data to be processed in inappropriate contexts. We do not accept that and believe that the formulation above makes a reasonable job of describing acceptable health-related purposes.

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.

ICO comment: Again, issues to do with the use of health data for medical research and for services such as cancer registration have often been contentious ones for us. So, it is welcome that, in short, this provision will make it clear that this is an acceptable additional use of health data.

Article 82
Processing in the employment context

1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

ICO comment: We are not clear as to the origins of this provision. We do not object to derogation here. However, any such rules must complement the provisions of the Regulation which should still apply fully in an employment context. However, that begs the question of how national law could add to the protection provided anyway by the Regulation. It is not clear what the "specific rules" might be. Clearly their introduction could cause considerable confusion for employers and employees alike.

Article 83
Processing for historical, statistical and scientific research purposes

1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:
(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

ICO comment: We welcome the clear privacy enhancing features of this provision. However, where there are large archives of paper records that contain personal data, for example, it may be impossible to either remove or anonymise the personal data or to keep the 'other information' separate. We would prefer an approach that also allows for restriction of access and security – plus a link to any effect on data subjects - as an alternative to the one set out.

2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:
(a) the data subject has given consent, subject to the conditions laid down in Article 7;
(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or
(c) the data subject has made the data public.

ICO comment: We have concerns around the requirement to verify and ensure the accuracy of the data contained in historical records, and the associated burden this would place on data controllers with large

collections of historical records, for example bodies holding archives. There should be no need to do this unless the data is being used to inform decisions about particular individuals.

Article 88
Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed.
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

ICO comment: We do not know if the government intends to repeal the UK DPA or whether it would retain those parts, for example s55, which are not covered by, and do not conflict with, the Regulation. Confirmation of the government's position on this would be useful. We are not sure of the legal propriety of reading references to the current Directive as being references to the Regulation, as at some points the two instruments say very different things. This would deal with the problem of loss of legal precedent though.