Castlebridge Associates

Submission to Department of Justice re: Proposed Data Protection Regulation

Castlebridge Associates | The Invent Centre, Dublin City University, Glasnevin, Dublin 9| www.castlebridge.ie| Phone: +353 76 6031850
Castlebridge Associates is a trading name of Bridgecastle Information Management Ltd
Registered in Ireland: 473477| Directors: Daragh O Brien BBLS (Managing Director), Colin Boylan BA MSc (Non-Executive)

Contents

About Castlebridge Associates

Castlebridge Associates (www.castlebridge.ie) is a leading consulting, training, and services firm that provides assistance to organisations in the Public, Private, and Not-for-Profit sector with their Data Protection, Information Quality Management, and Information Governance challenges in Ireland, the US, the UK and elsewhere.

We are a FETAC accredited training provider.

Our founder, Daragh O Brien, is a Certified Data Protection Practitioner, an Information Quality Certified Practitioner, a Fellow of the Irish Computer Society, and a former Director of the International Association for Information and Data Quality. He holds a degree in Business and Legal Studies from UCD and has lectured on Legal Regulation of Information Systems on the European Masters in Business Informatics in Dublin City University.

Daragh is the author of two books on strategy for Information Quality and Data Governance, including Data Protection. He is regularly asked by Irish and International media to comment on stories in the Data Protection and Information Quality area.

To contact us

Web	www.castlebridge.ie
Email	Daragh@castlebridge.ie
Phone:	**+353 76 6031850/ +353 87 6349125**

Introduction

The European Commission's proposed Data Protection Regulation is a development which Castlebridge Associates broadly welcomes. We provide training and consulting services in the areas of Data Protection, Information Governance, and Information Quality Management and see the general thrust of the Regulation as further highlighting the complimentary nature of our areas of strategic focus. In particular we welcome the standardisation of the Data Protection framework across the EU27 by way of the Regulation and would view this as facilitating the export of some of the training, consulting, and web-based services which Castlebridge Associates is in the process of developing to organisations within the EU27 and elsewhere.

However, our support for the Regulation is not without concerns, questions, and requests for clarification to be provided in a number of areas. Amongst other factors, we would be concerned that, without these concerns, questions, and requests for clarification being addressed prior to the Regulation coming into force that the potential cost savings and other benefits which might accrue to organisations from the Regulation could be significantly undermined through onerous increases in the cost of compliance. The approach to enforcement of the Regulation we feel needs to be aligned with the principles of Quality Management.

We would also be of the view that there is risk, given the level of prescriptiveness within the Regulation in the context of the skills and role of the Data Protection Officer, that a 'cottage industry' may emerge in the provision of training and consulting services for Data Protection Officers. We would be concerned that this 'cottage industry' would be largely unregulated as regards the specific qualifications and experience required for advisors and the quality assurance of any training and accreditation that might be delivered for Data Protection Officers. Without such a benchmarking capability for training and professional advice organisations will not be able to reliably judge the appropriateness of the skills and qualifications held by DPOs or firms or individuals providing such training or related professional services consultancy.

The remainder of this submission will examine in detail those areas of the Regulation which we welcome and support and outline why we welcome them as well as expanding on those areas where we would have concerns about the approach of the Regulation or the practicalities of actually implementing the Regulation in businesses and non-commercial organisations.

An uncomfortable imbalance between Prescriptiveness and Vagueness

As general point we feel that the Regulation (and the associated Directive) overall suffer from a distinct lack of specificity in a number of key areas. Key concepts are not clearly defined. New areas and new concepts are defined using synonyms and homonyms which will only serve to undermine practical application of principles. The full practical implications of concepts such as the “Right to be Forgotten” and Data Portability do not appear to have been considered in the context of a ‘real world’ information and data life cycle.

In our view there is an over-reliance throughout the Regulation on delegated acts, often at key points where guidance and clarity is needed **before** the Regulation come into effect. In key areas the Regulation fails to provide sufficiently clear guidance as to the standards of care to be applied, the rules governing the application of a concept, principle, or penalty. Overall we would be concerned that there is insufficient clarity and certainty in the Regulation as it currently stands for us to provide advice or guidance to our clients as to the nature, scope, and extent of actions they would need to take or structures they would need to put in place to ensure compliance with the Regulation and assure that they are striking the appropriate balance between their legitimate objectives and the privacy rights of their customers, suppliers, and partners.

Notwithstanding that, we feel that the Regulation as drafted represents a valuable evolutionary step towards a new Data Protection regime in Europe and, should the necessary clarity and guidance be included and provided it will stand a good chance of achieving its objectives.

A shift in Emphasis in Governance?

Our reading of the various provisions in the Regulation that it represents a subtle but significant shift in emphasis on the approach to Governance and the nature of organisation culture and thinking about Data Privacy and Information Management in general. From the requirements for documentation set out in Article 28 to the Privacy by Design concepts in Article 33, to the creation of the role of the Data Protection Officer in Article 35, we welcome most of the fundamental concepts which are set out in this proposed Regulation. However, there are some areas where we feel that the Regulation either doesn’t go far enough or fails to provide sufficient guidance to enable organisations to actually understand what is required of them to be compliant and, by extension, makes it difficult for organisations such as Castlebridge Associates to provide clear advice on what changes an organisation would

need to implement in order to achieve compliance with the requirements of the Regulations. This lack of clarity in key areas seems to be balanced only by the creation of provisions for overly specific prescription by the Commission in other areas.

A disconnect: Resourcing of Data Protection Officers v Data Protection Authorities

One of the significant shifts in Governance requirements in the Regulation is the introduction of the formal role of a Data Protection Officer in organisations (we explore in a later section our observations on these provisions).

One of the key provisions in relation to the Data Protection Officer role in an organisation is that the Data Controller or Data Processor is required under Article 36(3) to ensure that the Data Protection Off nicer is provided with "staff, premises, equipment and any other resources necessary" to carry out their duties and tasks. *There is no Article within the Regulation placing an equivalent duty on National Governments to ensure that the Data Protection Authority (in the case of Ireland the Office of the Data Protection Commissioner) has appropriate staff and resources to execute the responsibilities of the Data Protection Authority.*

While this may be an oversight on the part of the drafters or an omission based on the assumption that the obligations on Member States under Article 16 of the Lisbon Treaty addresses the need to require Member States to adequately and appropriately resource, staff, and fund their national Data Protection Authorities, in our view it is not appropriate that a greater burden is placed on Data Controllers and Data Processors than on National Governments in the context of properly resourcing the operational structures for ensuring compliance with Data Protection rules.

This disconnect is even more pronounced when one takes into account the greater burden that will be placed on the Office of the Data Protection Commissioner with the likely increase in use of Codes of Conduct, requests for Prior Authorisation and Consultation, management of Data Security Breach notifications, as well as the increased requirement for mutual assistance of other supervisory authorities. And into this mix we need to add the presence in Ireland of a large and growing number of large scale data-driven businesses such as Google, Twitter, Facebook etc. all of whom fall under the remit of the Irish Data Protection Commissioner.

If the intent of the Commission is to promote in Data Controllers and Processors a strong cultural shift away from 'tick box' compliance with the Data Protection principles towards a

culture of investment in and recognition of the value of effective and balanced management of the Data Privacy rights of individuals, then it is essential that the Commission and National Governments put their money where their mouth is, so to speak, and demonstrate a consistent and congruent shift in the culture of resourcing of and support for national Data Protection Authorities to ensure that they have appropriate operating structures, staff skill sets, access to additional resources and skills, and sufficient budget and financing to effectively execute their oversight and enforcement roles and support Data Protection Officers in executing their duties under the Regulation.

It makes little sense to introduce a formal level of governance in organisations without ensuring that they can get timely and effective responses and appropriately skilled support from the relevant National Data Protection Authority and the lack of headline investment and resourcing does nothing to communicate to the Executive leadership of organisations that Data Protection is anything other than another ‘fad’ which can be appropriately addressed through lip-service and ‘window dressing’ of management structures.

This investment in the Data Protection Commissioner must address staff numbers, training and skills development, review of operational structures and organisation design (such as a move from the the current ‘centralised decentralised’ model where majority of staff are based in Portarlington to a regionalised model where satellite teams can perform audit and review on a Regional basis (similar to Revenue’s Regional model) which would increase the perceived risk to organisations of being audited or investigated in person), the use of outsourced service providers to supplement core DPC resources for both IT review and Information Governance assessment, as well as financial resources. In this context a balance must be struck between the potential for the ODPC to become self-financing through the ring-fencing of fines and penalties for the use of the Commissioner’s Office and the need for the ODPC to maintain an impartial and objective advisory role in helping organisations be compliant with the law on Personal Data Protection/Privacy.

Care must be taken to ensure that the ODPC is seen as a benevolent traffic cop (directing people towards compliance, but with strong enforcement powers) rather than a malevolent clamper (seeking to hit revenue targets through their clamping activities).

Joseph Juran, the famous Quality Management thought leader, repeatedly admonished management and legislatures for believing that lip-service and the trappings of quality culture change would be sufficient. Without proper resourcing of Data Protection Authorities

being a **requirement** under the Regulation, there is no guarantee that National Governments will act any differently to business leaders who might lack an appreciation of the value of Data Privacy when there is a need to invest in improving the Quality Management System related to the Protection of Personal Data.

National Governments must be required to ensure the adequate resourcing of their Data Protection Authorities or the role of Data Protection Officers will be significantly undermined in practice. Lip service to the importance of Data Protection must be matched by resourcing, skills development, and funding to ensure the objectives and duties of the Data Protection Authorities can be achieved.

Replacement of Registration with DPC with formal documentation requirement

The removal of the formal requirement for Data Controllers and Data Processors to register with their national Data Protection Authority is a move which we welcome. The current situation under the Data Protection Acts contain a significant number of exemptions to this requirement which made this requirement essentially meaningless for the vast majority of organisations who are processing personal data.

We welcome that this externally focussed gesture of compliance has been replaced with a requirement under Article 28 for Data Controllers and Data Processors to maintain "documentation of all processing operations under its responsibility". This requirement reflects good management practice and best practices in the areas of Information Governance and Information Quality. As W. Edwards Deming (the man who brought Total Quality Management to Japan) famously wrote: "If you can't describe what you're doing as a process you don't know what you are doing". A properly documented process, with clear indication of roles, responsibilities, decision rights, and data movements is invaluable in identifying risks, applying controls, and ensuring that data is only processed safely and securely in a manner for which it was captured.

Our experience, and the international experience of organisations who have documented the processes their management of information and data, is that this simple act can help organisations unlock significant cost savings in terms of removing non-value adding process steps, reducing duplicated data storage, and improvements to the quality of the information to improve return on investment in managing that data.

The 250 Employee Threshold

However we would question the crude instrument that is applied to the threshold at which this requirement kicks in. Restricting the formal application of this to organisations with over 250 employees makes little sense given that all organisations benefit from having documented processes for a variety of reasons:

- Staff training
- IT Systems development/purchasing/support
- Enabling disaster recovery planning and Business Continuity planning
- Support change management
- Support staff skills development planning
- Staff succession planning
- Dealing with staff turnover, illness, retirements
- Ensuring consistency of customer service
- Identifying duplicate processes or opportunities to reduce costs by optimising processes.
- Risk Management

Process documentation is a fundamental component of any Quality Management System. Protection Personal Data Privacy is one goal which is met through an effective Quality Management System for Information. The risk inherent in 'hard coding' a staff size threshold into the process documentation requirement is that it sends a (we assume unintended) message to organisations that the documentation of processes (whether for Data Protection or other reasons) is only something that applies to Big Business, which could be at odds with requirements which may exist under other Irish or EU legislation.

Other sectors have requirements for organisations to document processes for Compliance or Quality assurance purposes. For example, organisations who are registering with FETAC are required to document an extensive set of processes for their Quality Management System for training delivery and evaluation. This requirement exists regardless of organisation size. Castlebridge Associates has been through this and we found that the focus on our processes helped us refine how we manage the training aspects of our business. While we aspire to having 250 employees we are still quite some way off that threshold.

The 250 employee threshold is a concern in other h of the Regulation as we feel it is a yard-stick that does not reflect the reality of data processing or modern business practices.

Standard Forms for Process Documentation

Article 28(6) states that

"The Commission may lay down standard forms for the documentation referred to in paragraph 1"

We are of the view that this wording is unnecessary and unhelpful and that the adoption of such a power by the Commission represents an excessively bureaucratic structure which would be burdensome to organisations who either have already extensively documented their processes using an existing industry methodology or an existing software tool. The Business Process Modelling/Management market is increasingly mature and Open Source tools are increasingly available.

For companies who have invested in Process Modelling/Management tools, we would be concerned that an overly prescriptive approach by the Commission would negate the benefits of any standardised Process Repository that the organisation might have developed by, inadvertently, making the tool no longer 'fit for purpose' and requiring the organisation to invest in a new Process Repository platform and to migrate their existing processes to this new repository.

For companies who have invested in the application of an industry standard process modelling methodology (e.g. Business Process Modelling Notation) there is an equivalent risk that an overly prescriptive approach from the Commission could undermine or negate any existing process documentation which the organisation may have compiled. While continuous improvement is an essential component of good practice in Process Management, being required to implement 'paperwork changes' without a clear value to the organisation will be met with resistance and will lead to increased costs and decreased morale in organisations that have been proactive in this space.

Simply put: There are any number of well-developed and well adopted Business Process mapping and documentation methodologies and toolsets. It would simply not make sense for the Commission to adopt prescriptive requirements as to the form of process documentation. What **does** make sense in this context would be for the Commission to instead focus on the definition of broader principles and practices for good process documentation to promote legibility of processes and ensure completeness of the process documentation. These should be published and adopted in the form of **guidelines** for what process documentation should include not prescriptive forms and formats.

The enumeration of documentation content set out in Article 28(2) to our view represents a substantially complete listing of factors to be considered in the definition of Data Processing processes. Beyond this the Commission should focus on setting objectives and providing clarification of and prescription of the **function** of process documentation (i.e. what the process should be capable of communicating, the broad objectives) rather than the **form** of the process (i.e. templates, notation etc.).

The Role of the Data Protection Officer

The creation under Article 35 of a formal Data Protection Officer role is a development that we welcome as it effectively puts a good governance practice which we recommend to clients on a statutory footing. However we have a number of concerns about this proposal which we feel need to be addressed before the Regulation is introduced.

Independence, Liability, and Whistle-blower Protection

The Regulation calls for the creation of an independent Data Protection Officer role. This independence is set out in Article 35(6), Article 35(7) and Article 36(2). The structures outlined within the Regulation provide for a suitably clear segregation of duties between the Data Protection Officer role and other management functions and is to be welcomed.

However, this independence would appear to bring with it the requirement for the Data Protection Officer to act as a fully independent advisor to the management function of the organisation, albeit in some scenarios as an employee of the organisation. This independence creates the potential scenario where the management team of an organisation may choose to ignore the recommendations of a Data Protection Officer or fails to properly resource the role. The DPO would appear to be required to report this to the National Data Protection Authority – in effect becoming a Whistle-blower.

However there is currently no statutory protection for Whistle-blowers in Ireland and, other than requiring that the DPO's role is for a minimum period of two years, the Regulation provides no further protection to the holder of that office in an organisation, be they an employee or a contractor. This could result in Data Protection Officers who do report instances of non-compliance with the Regulation being subjected to actions which affect their careers in organisations outside of the Data Protection role or which damage commercial relationships outside the Data Protection Officer role. It could also lead to Data Protection Officers not reporting issues due to a fear of such indirect impacts on their career or commercial relationships with client organisations.

A related weakness in the Regulation is with regard to the liability which Data Protection Officers may be exposed to by reason of giving advice or performing monitoring and oversight functions with the organisation that is Data Controller or Data Processor. To put it bluntly: As currently drafted the Regulation provides no protection for Data Protection Officers from litigation from their employers arising from errors or omissions in the advice given or in the conduct of their professional duties. This would have the effect of making it distinctly unpalatable for staff being assigned such a role to take it on given the potential risks involved.

What is required here, in our view, is that the Regulation either provides for all persons holding or performing a Data Protection Officer role to hold appropriate Professional Indemnity Insurance, or that the Regulation makes a provision similar to Section 45 of the Freedom of Information Act 2003 and Notice Number 7 (Protection for Civil Servants against legal actions in respect of the contents of documents created in the course of official duties) to indemnify or otherwise protect Data Protection Officers, their staff, and any contractors who they may engage, from liability arising from the conduct of their duties where:

1. Those duties were executed in good faith and with best efforts without improper or ulterior motives.
2. The Data Protection Officer, staff member, or contractor has made all reasonable efforts to attain and maintain an appropriate level of professional skill and knowledge in relevant and appropriate areas
3. Evidence of the operation of internal controls can be produced which demonstrate good faith basis and application of appropriate knowledge and skill.

As currently drafted the Regulation creates an unpalatable proposition for almost anyone performing this function where on one hand they appear to be compelled to give advice, monitor the functions of the organisation, challenge the leadership of the organisation, promote culture change in the organisation, and report breaches of the Regulation to the DPC without **any** substantive protection for them, their professional reputation (where advice is ignored or over-ruled by management), or their personal finances (should they find themselves being sued). In that context the role of Data Protection Officer becomes a poison chalice which no sane person would willingly accept and we would foresee organisations being unable to recruit for such positions as people would opt-out based on legal advice they might seek themselves.

The personal experience of our Managing Director, Daragh O Brien, in implementing and managing Regulatory Compliance structures has been very clear that without a statutory basis for the “mandate from God” and sufficient clarity of independence and immunity from liability (so long as you are following good practice) it is effectively impossible to achieve anything other than lip-service engagement with the necessary culture change. As such, without clear protection for Data Protection Officers who ‘blow the whistle’ or who give the best advice they can but make a mistake, the Regulation as currently drafted could have the unintended consequence of setting people up to fail rather than establishing a defined, respected, and independent tier of the Governance framework in any organisation.

Appropriate protections need to be introduced either in the Regulation (the ideal situation), through a delegated act of the Commission, or in National law. Article 37(2) allows for this type of provision by way of a delegated act of the Commission but it would be better, in our view, that the Regulation make clear reference to the protection of the Data Protection Officer in the context of independently reporting their employers for breaches of the Regulations and in the context of legal liability for acts, advice, or other factors in the performance of their duties.

Training, Certification, and Accreditation of Data Protection Officers

The Regulation requires by implication that Data Protection Officers should be appropriately trained and requires that they should possess a range of (unspecified) "professional qualities" as well as an "*expert knowledge of data protection law and practice, and ability to perform the tasks referred to in Article 37*" (Article 35(5)).

We feel that this provision is necessarily vague in the context of the Regulation but inoperably woolly in the context of organisations being able to define role profiles, validate relevance and levels of experience, and, for want of a better expression, being able to ensure they have the right person with the right skills for the job.

In particular, while Article 37 would appear to envisage the Data Protection Officer as being in an oversight and policing role, we feel that this is both infeasible in practice (where the Data Protection Officer will invariably have to be 'hands-on' in leading some or all of the activities, not just monitoring them) and does not align with the best practice models in Information Governance and Information Quality all of which reflect and recognise that effective governance of a Quality System requires some level of 'hands-on' interaction by the Governance or Quality teams in the definition of and evaluation of processes, controls, procedures etc. It also does not align with the likely role of the DPO in leading (rather than just monitoring) Privacy Impact Assessments.

By way of comparison, the International Association for Information and Data Quality (IAIDQ – www.iaidq.org) recently launched a professional qualification for Information Quality based on an exhaustive global study of the jobs people were performing and how they were performing them in the areas of Information Quality and Information Governance which found that practitioners were engaging in both strategic level over-sight and operational level development and execution of projects. This study resulted in a certification syllabus which spans a total of six distinct knowledge domains, with Quality Management principles being just one knowledge domain. Details of the IQCP certification can be found here: http://iaidq.org/iqcp/iqcp.shtml

Article 35(5) would also appear to suggest that the level of knowledge and skill which would be required to be a Data Protection Officer would be determined in accordance with the nature of the processing and the level of protection required for the personal data being processed. We feel that this would lead to undesirable unintended consequences should

Data Protection Officers move organisation from an area of low risk processing to an area of higher risk. We would recommend that the Regulation would require that Data Protection Officers have a minimum standard skill set commensurate with their role as an internal advisor to an organisation and that any industry sector specific 'add-ons' qualifications or courses provide the granularity to reflect the specific needs of a particular industry sector or particular type of processing. In effect the Commission is creating a new professional function and as such it needs to create an entry-level standard of knowledge and/or professional experience for people who will be holding this role, regardless of the nature, scale, or sensitivity of the data processing activities they will be overseeing. This is related to a significant degree to the point we made earlier regarding the risk of personal liability for Data Protection Officers and how that can be mitigated.

We would suggest that, **prior** to the enactment of the Regulation the Commission set out a clear set of criteria for what they believe to be the appropriate educational syllabus and skill set for a Data Protection Officer. We believe this would be permitted after the implementation of the Regulation under Article 35(11) but we would call on the Commission to publish drafts of any such criteria as soon as possible. Once such a core syllabus has been published we would call on the Minister for Justice and the Office of the Data Protection Commissioner to immediately request that FETAC develop a Special Purpose Award at Level 6 on the National Qualifications Framework to reflect the requirements of the Commission as well as the broader skills that would be required for a Data Protection Officer to perform their role effectively.

Should the Commission fail to publish a syllabus and required skill set, we would call on the Minister and the Office of the Data Protection Commissioner to request that FETAC begin as soon as possible to develop a Special Purpose Major Award at Level 6 on the National Qualifications Framework which will provide a benchmark for accreditation of and validation of Data Protection Officer skills by employers and the Data Protection Commissioner, and which would provide a standard of care which would contribute to any indemnification against personal liability which a professional Data Protection Officer might wish to avail of.

As an aside to the discussion of the Regulation we would also recommend the creation of a standard Data Protection basics syllabus by FETAC at Level 5 on the National Qualifications Framework for any person engaging in activities related to the processing of personal data (e.g. marketing professionals, IT developers etc.) which would be similar to the Safe Pass scheme which operates in the Construction sector. We feel that this would provide a robust

independent benchmark for the knowledge of Data Protection which an individual worker possesses and would help raise standards of professionalism in the area.

Validation of Training by means of Quality Assured Certification

Related to our previous discussion of the need to ensure that there is appropriate training and certification for Data Protection Officers and our suggestion that there be a role for FETAC (or their replacement entity) in supporting this objective, we are of the view that an opportunity has been missed with the current wording of Article 39 of the Regulation to introduce standardisation of or at the very least the ability to benchmark training courses, training providers, and the qualifications awarded.

We feel that Article 39 should allow for the Member States and the Commission to establish formal certifications or syllabuses of skill and knowledge for Data Protection Officers within the context of EU Data Protection principles the delivery of which would be through a properly quality assured certification process.

While efforts to certify organisations are to be welcomed and applauded from the point of view of encouraging compliance and promoting transparency so that consumers can compare service providers, the Regulation provides no such mechanism for organisations to benchmark and compare the skills, knowledge, and experience of staff who will be involved in either executing or overseeing the processing of personal data.

Article 35(5) of the proposed Regulation sets out that the level of skill and experience required by a Data Protection Officer should be defined with reference to the processing being carried out in the organisation. We would suggest that the transparent and reliable comparison and benchmarking of the skills of potential Data Protection Officers would require two levels of standardised awards, a FETAC Level 5 minor award on basic principles and a Level 6 Major award covering more advanced topics and the wider skillset necessary for effective Data Protection Officers to operate effectively in larger organisations or in more complex processing scenarios. Ideally this standard syllabus and skills framework could be developed as a pan-European model.

In particular, in the context of potential personal liability of Data Protection Officers in the conduct of their duties, it is important that appropriate and sufficiently benchmarkable standards of knowledge can be demonstrated. The alternative is to risk having to have the

Courts make determinations on the suitability of knowledge possessed by a Data Protection Officer.

Note that we are not calling on the Commission or the Department to define specific courses but rather engage FETAC to have a defined set of learning objectives and objective assessment criteria developed to which private training providers (such as Castlebridge Associates) can adapt existing training or develop new offerings.

This would also have the additional benefit of ensuring that training will be delivered in a quality assured manner by approved quality assured trainers.

The Need to Assure/Ensure Quality of Trainers and Consultants

As a general comment we feel that the shift in Governance emphasis towards internal documentation and training as the keys to effective compliance introduces a risk that organisations may fall foul of unqualified or inexperienced consultants or trainers who see a new revenue stream in the demand for advisory, consulting, or training services.

Article 39 creates the option of creating privacy seals and certification for the Data Controller and Data Processor, but again we feel that an opportunity has been missed to provide equivalent mechanisms for trust, transparency, and benchmarking, of service providers in the professional services and training in a manner which would allow organisations and individuals to make objective comparisons of providers on factors other than price.

A similar model exists with FETAC which maintains a register of approved training providers for FETAC certifications.

As a firm providing training and in the area of Data Protection, Castlebridge Associates would have no objection to meeting reasonable requirements that might be met as regards our qualifications, experience, or quality assurance systems for our Data Protection services. However the requirements should not be defined in a way that precludes SME/Micro enterprises providing services in this space and should be defined in such a manner as to provide a level playing field for all participants in the market.

However, if Data Protection Officers are to rely on trainers or professional advisors in the area of Data Protection and related process and governance they must be able to do so in a way which provides them with an assurance that their advisors actually know what they are doing.

The 250 Employee Threshold

In the context of the Data Protection Officer requirement we are concerned that yet again a crude instrument is being applied to determining whether a Data Protection Officer is required in an organisation.

This 'head count driven' threshold does not reflect the way in which businesses increasingly process and utilise information and data, such as the use of outsourced providers. Small companies can process significant amounts of personal data. Cloud computing, outsourcing, and other resourcing strategies mean that the capital investment required to be a large processor of personal data (of which headcount is a proxy indicator) is no longer a valid indicator of size, scale, and risk. Furthermore the 'head count driven' threshold is one which would be trivial for an organisation to bypass and also could act as a disincentive to organisation growth above 249 employees (perhaps leading to complex organisation structures being put in place).

'Big Data' is an emerging term in data management, referring to the processing and analysis of very large data sets. Gartner Group has defined Big Data in terms of three key vectors: Volume, Velocity, and Variety. These vectors provide an increasingly industry accepted framework which could be easily applied to risk assessing whether a Data Protection Officer is required by an organisation.

- Volume: How much data is being processed
- Velocity: How often is it being processed? How often is it coming in or out of the organisation?
- Variety: What kinds of data are being processed?

By applying this kind of framework it would be possible for a more nuanced risk-based model for determining if a formal Data Protection Officer role is actually required based on the functioning of the organisation rather than its actual form and physical size.

We note that the Article 29 Working Party has made similar comments in this regard in their Opinion 01/2012 addressing the new Regulation and Directive.

In any event, Castlebridge Associates would be of the view that organisations should ensure there is a defined management role with responsibility for ensuring that Data Protection duties are appropriately complied with.

Changes to Penalties: An argument for a Data Protection Penalty Points Scheme

The proposed Data Protection Regulation introduces in Article 79 an array of new penalties at a level which should deter all but the hardiest and most reckless Data Controller or Data Processor.

Given the focus in the European and International media on the upper-end sanctions that are available we feel that the potential under Article 78 for the provision of lower-scale penalties for infringements has been missed and that there is clear potential for the development of a transparent 'sliding scale' scheme where lower end penalties can be levied by way of a fixed-penalty notice but where recidivist behaviour by an organisation (indicative of a failure in internal governance or organisation culture) would incur an increasing penalty up to a threshold where the maximum penalties would be applicable.

The adoption of a fixed-penalty notice approach with a graduated response for repeat offenders would, in our view, have the following benefits:

1. It would reduce the requirement for the Data Protection Commissioner to prosecute breaches via the Courts (but as with parking fines or offences under the Road Traffic Acts, the Data Controller would be entitled to appeal to the Courts).
2. It would provide a sliding scale of penalties which could be easily communicated and explained to business managers.
3. It would provide a simple ready reckoner for the bottom line impact of breaches of the Data Protection regulations which would help organisations make more balanced investment decisions
4. It would provide a structured and slightly more certain escalation path for the Data Protection Commissioner or other national Data Protection Authorities from the consultative support on a first offence through to the maximum penalties which can be applied.

We feel that the allocation of "penalty points" to instances of breaches of the regulations in a manner similar to the operation of penalty points schemes in Motor Vehicle offences would support a culture of continuous improvement, would feed into any validation and verification for a Privacy Seal, and if penalty points were cumulative and certain categories of offence resulted in points being applied for multiple years, would support the development of long-term culture change in organisations.

We feel that the adoption of this form of scheme at a European level by the Commission by means of a standardised “Penalty Point Scheme for Data Protection” would be the most effective means of achieving this, but we note the discretion that Member States have in this regard and we hope that the Department gives consideration to this proposal.

The Double Jeopardy Risk and Balance in One-Stop-Shop

We would be concerned that, given the lack of clarity around the practicalities of managing the enhanced co-operation and “one-stop-shop” aspects of the Data Protection Authorities under the Regulation (as outlined by the Article 29 Working Party in their Opinion 01/2012) there is a distinct risk of double-jeopardy arising where a Data Controller or Processor is engaged in activities which result in complaints arising from more than one jurisdiction and administrative enforcement actions being taken by more than one Data Protection Authority.

The “One-Stop-Shop” concept must operate for the benefit of both the Data Controller/Processor and the Data Subject in making things simpler and more straightforward. However, as currently drafted there is significant lack of clarity of how these mechanisms will actually work. This creates legal uncertainty, but even more damaging it creates uncertainty about the structures organisations will need to put in place or the likely cost of compliance. There is a significant difference in economic impact for an Irish SME dealing with the Irish Data Protection Authority with regard to a complaint which emerged via the Italian Data Protection Authority as opposed to having to deal with the Italian Data Protection Authority.

In light of these concerns we would ask that the relevant Articles and Recitals of the Regulation be reviewed to ensure balance and legal certainty.

Biometrics, Monitoring and Profiling, and definition of Personal Data

Castlebridge Associates is of the view that there are a number issues with the definition of biometric data, monitoring, and systematic monitoring in the Regulation which need to be clarified to improve certainty for Data Controllers, Data Processors, and Data Subjects. Given the extensively prescriptive nature of the Regulation it is essential that fundamental issues such as the definition of core concepts and the definition of 'business rules' for required governance models and roles are defined with minimum scope for ambiguity.

Biometric Data

We would echo the Article 29 Working Party's opinion on the definition of biometric data in Article 4(11) of the Regulation. We welcome the fact that there is now a definition. However we would be concerned that the current wording over-emphasises the use of biometrics to identify an individual person. A more common use of biometric data is to support authentication. We feel that the definition as currently drafted needs to provide more clarity as to the **form** that biometric data may take (i.e what kind of data could be considered biometric data) rather than the **functions** that that data may be used for.

Notwithstanding that need for clarity, it is important that the definitions which are provided are not overly prescriptive so as to allow for the evolution of new types of biometric data types and potential future uses.

Monitoring and Profiling

We would consider the wording of Article 20(1) to be insufficiently precise. As currently drafted it is insufficiently clear whether the use of web analytics tools, user tracking, email open tracking or click through, social media click through measurement, development of location based profiles by mobile applications, or social media profiles fall within the scope of Article 20.

Our concern is further compounded when Article 20 is read in parallel with Article 35 (creating the requirement for Data Protection Officers in certain circumstances). Article 35(1)(c) requires that entities who are engaged in "regular and systematic monitoring of data subjects" must appoint a Data Protection Officer.

The meaning of "systematic monitoring" is not defined anywhere in the Regulation. As such, it could be argued that this is a form of profiling. Therefore the imprecision of the definition of what constitutes "profiling" could contribute to a lack of clarity as to whether or not a Data Protection Officer is a mandatory requirement for an organisation or not.

If web analytics, user interaction tracking, email open tracking or click-through tracking etc. are included in the scope of profiling than it is arguable that any organisation who is making use of email marketing or is measuring marketing campaign success based on click throughs on to a website would require a Data Protection Officer.

Definition of Personal Data

Castlebridge Associates must question the decision by the Commission not to adopt the already published and established definitions of Personal Data as contained in Opinion WP136 of the Article 29 Working Party. Given the extent of other changes that are being introduced in the Regulation we feel that at least one fixed point from the current framework should be maintained. The fundamental definition of Personal Data is one such fixed point in our view.

We would suggest that Article 4(1) and Recitals 23 and 24 of the Regulation be amended accordingly.

Furthermore, the definition as set out in Article 4 and the associated Recital would appear to limit the concept of personal data to scenarios where an exchange of monetary value for goods or services is taking place. We would submit that this needs to be reviewed to allow for situations where the item of value that is being exchanged is the data itself, for example for the purposes of availing of ‘free’ social networking tools where the customer’s data is the price of admission.

Main Establishment, Cross Border Transfers, and Nominated Representatives

We feel that there are a number of gaps and weaknesses in the Regulation as it is currently drafted that create a degree of uncertainty for Data Controllers, Processors, and Data Subjects that should be avoided.

Main Establishment

From our reading of the Regulation it contains a number of different definitions of business unit or legal entity in Article 4 which are insufficiently distinct from each other and to our mind appear synonymous, describing the same thing from different perspectives. This lack of clarity makes it difficult to determine the link that exists between the main establishment and the duties of the Data Controller.

There is no clarity as to how the 'main establishment' of an organisation would be determined. The Regulation appears to be silent on the question of whether the rule would apply to the disparate business activities of a multinational operating in multiple business sectors. The Regulation also does not appear to have considered the scenario of distinctly separate business entities entering a collaborative enterprise without a formal hierarchical organisation relationship (e.g. a consortium assembled to work on a particular project or develop a particular product or service).

As the concept of "main establishment" is a foundation of the mutual co-operation framework between Data Protection Authorities and affects the operation of any "one-stop-shop" for DPAs and Data Subjects, it is essential that the rules which will apply to the determination of main establishment are clearly defined.

The use of synonyms and homonyms in the definition of key concepts such as a business unit or enterprise does not lend itself to the level of clarity that is required.

To that end we would suggest that the definitions in Article 4 should be reviewed.

Cross Border Transfers

We would query the wisdom and practical enforceability of overseas transfer on the basis of instruments that are not legally binding. In our view this would potentially remove a key tool for dispute resolution and formal definition of roles, responsibilities, and duties.

We would ask that the practical intent and effect of Article 41(6) be clarified, particularly in light of the recommendations of the Article 29 Working Party in Opinion WP114 regarding the need to preclude derogations where overseas transfer is massive, repetitive, and structural.

Nominated Representatives

The provisions in the Regulation relating to Nominated Representatives also, in our view, require clarification on a number of fronts.

1. Clarity is required as regards the role, responsibilities, and potential liability of Nominated Representatives acting as agents of a Data Controller or Data Processor.
2. We would question the logic of applying a penalty to the Nominated Representative, who may simply be an entity providing Data Protection advisory services and a

contact point for the Data Controller but having limited decision making authority regarding the operation of personal data processing.

In an echo of our comments regarding the potential personal liability of Data Protection Officers earlier in this submission, we would submit that Nominated Representatives who engage proactively to advise their clients and who apply appropriate diligence and skill in their duties as Nominated Representatives to ensure compliance with EU Data Protection rules should have an indemnification from prosecution and penalty.

Similarly, some degree of “whistle blower” protection should be considered for Nominated Representatives who breach client confidentiality or other duties to notify a Data Protection Authority of breaches of the Data Protection Principles by their client.

Privacy Impact Assessments, Public Authorities, and Further Incompatible Use

Castlebridge Associates are of the view that the various provisions in the Regulation relating to Privacy Impact Assessments, the exemptions available to Public Authorities, and the concept of Further Incompatible Use require careful review to ensure that unintended consequences do not follow from the Regulation in practice.

Further Incompatible Use

We feel that the provisions of Article 6(4) create a significant potential for unintended consequences and impacts on Data Subjects in the context of processing both by Public and Private Sector entities, particularly if there is excessive reliance on the processing conditions of Performance of a Contract or Public Interest. We feel that, as drafted, the Article invites the risk of unwelcome and unpopular ‘scope creep’.

To borrow a quote from popular culture: “With great power comes great responsibility”. Article 6(4) provides a significantly enhanced power to Data Controllers, one which we fully recognise the need for in certain circumstances. However there is no guidance provided in the Regulation as to what those circumstances might be or any rules which might be applied to assessing whether a particular scenario is one in which the extension of use beyond the purposes for which data was originally captured.

To that end, we would ask that Article 6(4) be redrafted to be more aligned with the limitations set out in Article 21. We would also ask that, in redrafting Article 6(4), that the

Commission take account of the planned guidance on Further Incompatible Use which is scheduled in the work plan for 2012-13 of the Article 29 Working Party.

Public Authorities

We must echo the concerns of the Article 29 Working Party with regard to the exemptions proposed for Public Authorities. The introduction of exemptions under Article 9(2)(g) allowing the processing of sensitive personal data for tasks "*in the public interest"* creates the potential for a broad and minimally controlled changes in purpose for the use of personal data and sensitive personal data far in excess of what might be appropriate given the right to Personal Data Privacy in Article 16 of the Lisbon Treaty.

We feel that the various provisions in Article 6, Article 9, Article 17, and Article 21 which relate to Public Interest or similar exemptions should be reviewed to ensure that they do not create too broad a set of exemptions which would invite abuse or misuse by well-intentioned public servants.

As a general principle, Castlebridge Associates would be concerned that an overly broad set of exemptions for Public Authorities, combined with an even more relaxed framework in the Directive relating to Law Enforcement could effectively create a Three Tier Data Protection regime within the EU, with private enterprise being held to a greater standard of care despite there being a potentially greater scope for misuse or abuse of personal data privacy by Public Bodies. Such a "Three Tier" regime would run counter to one of the stated reasons for the review of Directive 95/46/EC – to ensure comprehensiveness and reduce variation in Data Protection rights, responsibilities and duties within the EU.

We would also be of the view that the wording of Recital 18 should be reviewed to make more explicit the relationship between and need to strike a balance between Data Protection and Freedom of Information rights.

Privacy Impact Assessments

We welcome the introduction of Privacy Impact Assessments as a formal tool within the Regulation. However, we feel that for them to be truly effective the Commission must, yet again, tighten up the definition of a fundamental concept: Privacy by Design. The definition in Article 23 should be expanded on in a specific Recital given that it is now a fundamental principle of Data Protection within the EU.

We feel that the requirement under Article 33 to conduct a Data Protection Impact Assessment needs to be reviewed to ensure that the level of assessment that is performed in each case is appropriate to the nature of the processing, the scale of the processing, and the level of risk to the data. What must be avoided at all costs is the evolution of a “Check Box” approach to Impact Assessments which is a demonstrable risk in other areas of Regulatory Compliance and Quality Management.

Tick box driven Privacy Impact Assessments, driven solely off documentation and process flows may suit certain low complexity/low risk processing scenarios but the Regulation needs to ensure that any “Check List Manifesto” that might emerge be defined in such away that it can drive more indepth and introspective analysis of processing, particularly given the trend to “Big Data” and increased data sharing between public sector and private sector organisations.

Finally, we would ask that the exemption from conducting Data Protection Impact Assessments that Public Authorities can avail of under Article 33(5) be reconsidered or at least limited to scenarios where the process of developing the legislative provision which is being relied on as the basis for the exemption has adequately addressed the requirements of the Data Protection Impact Assessment and a clear implementation plan for processes, policies, protocols and controls is set out in the legislation.

The Right to be Forgotten, the Duty of Transparency, Data Portability

No discussion of this Regulation would be complete without a discussion of the Right to Be Forgotten and the new Duty of Transparency. Both of these concepts are welcomed but we have concerns that they both need clarification as to their practical application and effect.

Right to Be Forgotten

The Right to be Forgotten creates an array of practical and pragmatic challenges through the life cycle of information. One key concern which we would have based on our reading of the Regulation is that it appears to be defined from a world view in which the Data Controller in a given circumstance is only engaging with downstream “consumers” of data they provide.

Reality is often more complex and the Regulation does not appear to allow for or require a Data Controller who has obtained data from a supplier of data (a partner, a list broker etc.) to notify that upstream provider of a request to be forgotten. Related to this is what we feel is a

lack of clarity as to what it is that people are asking to be forgotten for... is the right to be forgotten linked to the context of a purpose or a use (e.g. “I want to be forgotten for direct marketing for lawnmowers”) or is it, **in all cases**, an absolute request?

We feel that, given the array of potential scenarios and the variety of opinion and comment on the nature and scope of this right that the Commission should revisit the wording and ensure that the Regulation is appropriately clear as to what the scope and implications of this Right are.

The Duty of Transparency

Article 11(2) of the Regulation requires that information about and communication of or relating to the processing of personal data should be in an “intelligible form” that is “adapted to the Data Subject”.

We feel that this Article is insufficiently clear as to the nature and scope of the obligation that is being placed on the Data Controller or Data Processor in this context.

1. What is ‘intelligible’? What objective operational definition is provided of this term?
2. What is the limit, if any, to the Controller or Processor’s obligation to adapt the information they are providing to the needs of the Data Subject
    a. Do they need to provide the information in Braille or audio for vision impaired customers?
    b. How many languages should they provide the information in?
    c. Would ‘staggered/staged’ communication of purposes etc. be sufficient (for example where a customer had to sign up separately to additional services offered by a company)?

The extent and scope of this duty needs to be addressed in the wording of the Article. We would suggest this alternative wording:

“*Insofar as is reasonable with regard to balancing costs to the Controller and the achievement of the objectives of this Regulation, 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”.*

Data Portability

While it would seem from the various briefings that have occurred in relation to this Regulation that the focus of the Data Portability obligation is primarily on Social Media and similar Cloud-computing scenarios, we feel that the Regulation as drafted creates a much

broader right which could give rise to issues in the context of customer migrations co one service provider to another, particularly in the context of telecommunications service provision.
This would potentially constitute a massive transfer of data, some of which may be of a sensitive nature (e.g. comments in CRM systems relating to customer complaints and internal operations) and which may contain personal data of other parties (e.g. contact details of staff members who were dealing with a complaint.

We would ask that provision be made in the Regulation to limit the scope of data that would need to be provided in defined circumstances such as that which is outlined above.

The Directive and relationship between Data Controllers and Law Enforcement

The Regulation as currently drafted and the associated Directive for Police and Law Enforcement would appear to create some undesirable challenges for Data Controllers and Processors who, for whatever reason, must interact with and share information with Law Enforcement or similar entities.

We would echo the Article 29 Working Party's comments on the Directive, in particular its distinct setting of a lower standard of care for Law Enforcement with regard to some of the fundamental principles and some apparent contradictions between the Regulation and the Directive with regard to lawfulness of processing and the overly broad exemptions that are provided for in the Directive.

In particular we would be concerned that Data Retention is not addressed, but we acknowledge that this may be due to the pending ECJ litigation challenging the Data Retention Directive.

Adopting Quality Principles

While not an element of the Regulation or the Directive *per se* Castlebridge Associates' involvement in Information Quality Management consulting and training prompts us to ask whether, given the shift to an internal focus on documentation, impact assessment, governance, and other characteristics of Quality Systems frameworks, whether the enforcement of Data Protection regulations might move to allowing statistical evidence of the

operation of processes and controls to be provided and reviewed as part of the investigation of complaints and the assessment of and levying of penalties.

This move to a systemic form of enforcement rather than a focus on ‘zero defects’ might result in a better adoption of the documentation and governance requirements of the Regulation, particularly in the SME sector.