

# **A comprehensive approach to personal data protection in the European Union: COM (2010) 605**

## **Comments by BT Group PLC**

BT thanks the European Commission for the opportunity to comment on its Communication on reform of the EU data protection framework. Our observations are provided mainly from the following perspectives, in the majority of which BT is also subject to the additional sector-specific data protection rules of the EU Directive on Privacy and Data Protection in Electronic Communications Directive (PEC Directive):

- BT is a major provider, in both the retail and wholesale sectors, of a broad range of electronic communications and value-added services in the UK, where we are one of the largest processors of personal data. In particular, BT Retail has over 13m consumer customers and over 1m small and medium business customers.
- BT is also increasingly involved in outsourced processing and storage of personal data for a broad range of business and governmental institutions. Customers include controllers of some of the EU's largest collections of sensitive personal data such as the UK's National Health Service. We are also a significant European and global player in the emerging cloud computing industry
- Finally, BT also provides networked communications and IT services to business customer sites in more than 170 countries, including all Member States of the European Union.

### Overview

The implications of various Treaty changes in combination with changes within the Commission in terms of “ownership” of the Directive, are complex and potentially far-reaching. We call on the Commission to engage with the full range of stakeholders affected by them – and who cannot be expected to be specialists in this field to ensure that these stakeholders can contribute meaningfully to development of the data protection system in the EU.

It is opportune to re-assess the role and relationship of actors such as the Article 29 Committee, EDPS and the Commission, and to ensure that their roles, interactions and degrees of independence are understood by other stakeholders

Conflicts or apparent conflicts between EU data protection legal requirements and information requirements under other legislation/regulatory regimes in areas such as financial services (e.g. whistle-blowing, Sarbanes-Oxley, Swift), transport (airline passenger data and law enforcement (pursuit of both criminal and civil matters) are increasingly commonplace. Such conflicts pose problems and risks for businesses caught in the crossfire and action that can be taken to reduce these would be welcome.

We consider that getting the balance right between “general” principles and more granular aspects is key to providing clarity and certainty – too much “generality” would

leave too much uncertainty and too much “granularity” would be too rigid. We are not sure that the review is consistent in seeming to pursue greater enforcement and flexible self-regulation simultaneously.

We consider that “privacy-by-design” should not be extracted and elevated to any kind of new, stand-alone and rigid principle which attracts specific enforcement. As indicated in our comments on post-1995 developments below, there is always a degree of unpredictability in technology and how people choose to use it. Expecting entities to anticipate all possible uses and abuses and design in from the earliest point possible how to address them would chill innovation and raise costs.

The fundamental principles of the current Directive must continue to play a central role in protecting European citizens’ rights as well as delivering effectively on single market goals, by curtailing and eliminating barriers which have been created in the way that a number of Member States currently operate their national data protection regimes

Since the Framework Directive was adopted in 1995, there have of course been huge developments in technologies and applications which involve the processing of data and in the extent to which citizens interact with, take-up and use them. Many developments arise from citizens’ own experimentation with, and deployment of, new technology and applications in ways which have not been anticipated by those who initially developed them. Initiatives that have begun at a very small scale (a few individuals only) and on a non-commercial basis may have become massively popular rapidly, and developed into commercial services, but it has been largely unpredictably if and when this may occur. In particular, the processing of personal data via the internet has increased exponentially, as have international data transfers, and many business models have emerged (and died). Outsourcing and sharing of physical and software resources by businesses and organisations of all sizes has become a common practice. There is a state of flux and evolution and this will continue for the foreseeable future.

BT considers that the fundamental principles of the EU Framework Directive remain basically sound and relevant irrespective of the developments indicated above. Indeed, it is important that the Directive retains these as a solid foundation, around which any contemplated changes are made. Rejecting them and starting completely afresh would be highly disruptive – creating new and prolonged uncertainty and lack of clarity for all.

However, we share the view of the Commission, the Article 29 Working Group and many others that there are areas where it has become increasingly difficult and complex to apply aspects of them in practice. This creates uncertainty and compliance problems which we would like to see diminished. Accordingly, we would support a move to an updated regime based on the following key elements (adopting where appropriate the order in which they feature in the Commission document):

- a breach notification requirement only with appropriate thresholds for notification;
- retention of broadly the same basic data protection principles, but subject to the clarifications we refer to in this response. In particular, in order to take account of technological developments and increasingly collaborative processing on a global scale, a thorough reappraisal is required of certain key concepts/ definitions (eg “*consent*”, “*controller*”, “*processor*” and “*personal data*”);

- elimination or drastic reduction of requirements for prior notification of data processing operations;
- simplification and streamlining of the rules governing international data transfers.

### Detailed comments

#### *Breach notification*

It is too early to assess the impact of the breach notification requirement in the PEC Directive, but it is clear that (notwithstanding the way in which the requirement is framed) different Member States are adopting different approaches in terms of the threshold for notification (and indeed on some other issues, such as whether the *risk* of disclosure can itself be sufficient to trigger the notification requirement and what sanctions can be applied following a notification).

This highlights the need for any *general* notification requirement to set parameters or guidelines for the types of breach that should be notified (eg *serious* breaches only, determined against certain criteria such as *potential harm*). Failure to address these issues will place an enormous burden on controllers and regulators alike, without conferring any meaningful benefit on data subjects.

#### *Consent*

The Commission's proposal to clarify the current rules on consent is welcome. However, whilst there may be arguments for strengthening them in particular cases, Commission should consider the case for different standards of consent or permission in different circumstances, whilst subject to an overriding obligation of transparency.

We make this point primarily in the context of our experience of the PEC Directive, but it is one that may be of more general application. For example, there is currently a debate, both within the Commission and the Member States, as to the appropriate consent required for the placing of cookies and similar technologies. It is not yet clear what will emerge from this, but it seems to be common ground that a balancing act is required, taking due account of the practical difficulties in obtaining individual, positive consents, the harm that may arise if they are not obtained, and the importance of cookies for the efficient functioning of the internet.

There are other examples where the threshold for consent should be considered afresh. For instance, under Article 5 of the PEC Directive, there are circumstances in which consent may be required from a website owner (as one of the parties to a communication). It is simply not practical (and is arguably incoherent conceptually) to seek a positive, informed consent. Given the way in which the world-wide web operates, it may be reasonable to proceed on the basis of an implied but rebuttable consent on the part of the website owner (subject to certain caveats).

In summary, whilst the need for transparency and consumer protection is widely accepted, it is not appropriate for the Framework Directive to adopt a one-size-fits-all requirement for consent. If it does so, there is a genuine risk that the effective functioning of the internet and the development of value-added online services will be undermined.

### *“Controller” and “Processor”*

The current definitions of ‘Controller’, ‘Processor’ and ‘Personal Data’ are more complicated in the light of technological developments, new business models and globalisation. In the case of cloud computing in particular, a reluctance by some service providers based outside the EU jurisdiction to recognise the functional approach to the allocation of responsibilities promulgated by the Article 29 Working Party in its Opinion 1/2010 on the definitions of ‘Controller’ and ‘Processor’, has resulted in contrived solutions to the allocation of responsibilities with no real certainty of the ultimate legal position.

Whilst cloud computing provides an obvious example of the potential difficulties arising from the controller/processor divide, it is by no means the only one. The notion of a processor (effectively as agent) simply performing a set of operations at the behest and instruction of a controller is largely an outmoded one. Commercial reality is now far more complex. Businesses frequently outsource a broad range of functions, such as Human Resources administration, where the outsourced supplier itself takes specific decisions on data processing on the basis of very general instructions.

So, whilst the current definitions were framed to enable a degree of flexibility, greater clarity is required: commercial undertakings need to be able to predict with some degree of certainty whether or not they have legal responsibility under the data protection regime. Accordingly, the Commission should review these definitions, taking account of the problems of practical implementation, and recognising that the competitiveness of EU service providers is also a factor to include in the balance of the equation.

### *“Personal data” and data subject access rights*

The definition of ‘Personal Data’ in the Directive is problematic and requires reappraisal and greater clarity. It is now broadly accepted that, on a purposive interpretation, information may amount to personal data if it relates to a *distinct* individual even if that person cannot actually be identified. This is counter-intuitive and has led to the need in certain instances to distinguish between “personal data” and “personally *identifiable* data”, but it is probably the latter concept that has more resonance with data subjects.

Technological developments (again) have given rise to a further issue. The concept of identifying “indirectly” means that information held legitimately on internet logs, for example, may fall within the definition of personal data. This is a specific example of a broader issue, namely that controllers (ISPs in particular) may hold considerable amounts of data that could in principle be linked back to specific individuals but which in practice are highly unlikely to be and which in any event are of little or no biographical significance. Accordingly, BT considers that there is a case to limit the scope of ‘indirect’ identification, or the scope of data subject access rights to ensure that those rights can be exercised in a meaningful and clear way but without placing excessive burdens on industry.

### *The notification system*

The current notification requirements are unduly burdensome, and in a world where businesses and many other organisations routinely process customer and employee data, achieve little benefit. BT accordingly queries the justification for the retention of a notification regime at all, but would certainly welcome revisions to the current regime which are less onerous and costly than the current one. We are wary that attempts at EU-level “harmonisation”, despite being well-intentioned all too often get bogged-down and lead to increased bureaucracy and costs. Consideration needs to be given to how mechanisms such as mutual recognition and notifications in a single MS in relation to all MS can be developed and instituted in this area as well as in relation to international transfers.

### *International data transfers*

The current mechanisms for international data transfers need to be improved. We note that for intra-Group transfers the BCR regime may be less onerous than it has been previously, but taken together with the model contracts regime, the system overall is unduly burdensome for controllers and regulators alike. Indeed it is arguably unsustainable, given that international data transfers have such a prominent role in the world today (and certainly one that was not foreseen when the Directive was first introduced). Simplification of the existing regime(s) for international transfers would be welcome as would the development of alternative mechanisms that are not reliant on prior permissions or notifications.

### *Applicable law*

The Commission’s proposal to revise and clarify the rules on applicable law is sensible. It would clearly be helpful if the approach ultimately adopted in the sphere of data protection is aligned with the approach adopted for other areas of law relating to cloud computing (eg. cybercrime). To the extent possible, coordination of the EU approach with the approach of other authorities at global level would be equally helpful.

The consultation refers specifically to cloud computing in the context of applicable law. Two of the keys to effective cloud computing are data back-up and server load balancing. In simple terms, this means that the same data may often be found in two places at the same time, and may be switched rapidly between servers on a regular basis. An approach focused on the geographic location of specified equipment is consequently unlikely to provide an answer to current problems.

### *“The right to be forgotten”*

BT has concerns about the proposal to introduce this broad, new right. Further clarification and scoping is required before we can comment substantively. In particular, we would be interested to learn to what extent and in what contexts the existing data protection principles (especially the fifth principle) are considered to offer insufficient protection.

We acknowledge that the issue of what constitutes *legitimate* processing may require review and clarification, particularly in the light of new models (eg social networking), where the sharing of personal information is an intrinsic feature. However, any notion of “the right to be forgotten” would need to accommodate a broad range of exceptions.