



**Symantec Response to EU Commission Consultation on the Legal Framework for the
Fundamental Right to Protection of Personal Data**

1. Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation

In 1995 the Data Protection Directive (95/46/EC) was introduced into an era preparing to embrace convergence and the rise once more of the Internet following the dot.com boom and bust era. This was also a time when closed, nationally protected computer networks and systems were the norm. However, in the fourteen years that have since passed European citizens, industry and governments alike have become increasingly reliant on the Internet, mobile telephony and advanced communication infrastructures to communicate, live, work and play. This has raised new opportunities for all as well as increased challenges for the protection and privacy of personal data in the online, and offline, worlds. Today the very foundations of Europe's modern society and economic stability are built on electronic communication infrastructures that span across national, European and international borders and the data that is shared, processed and stored within these networks.

Since 95/46 Directive was passed the way in which information and data is used, processed, accessed, shared and stored has certainly changed. In the past when less information was required, and therefore gathered, information enjoyed relative privacy due to its obscurity locked in filing cabinets or even held within an organisations internal customer spreadsheet stored on a single user's desktop machine. With the pervasive nature of technology and the global flow of data, information has lost much of its obscurity leading data to become the currency of the digital age; needed to access goods and services online and easily shared. Information currently moves around the globe at light speed, duplicated at literally no cost and once information is set free it is hard to control and almost impossible to delete.

Clearly the way in which data flows has and continues to change. The current reality where data moves between organisations and around the world seamlessly, simply at the click of a button, could not have been fully realised when the Directive was introduced back in 1995. Information now flows not only between various organisations as well as European Member States but more importantly between EU and non EU states where different global jurisdictions means there may often be varying degrees of data protection legislation and regulations in place. This raises legal challenges for organisations operating in multiple jurisdictions but also risks to the level of protection given to personal information. While it is important to review the effectiveness of Directive 95/46 for data protection within the EU it is also considered equally important that any review of the Directive address the need to ensure information being transferred outside the EU is also fully protected and secure.

The world today is very different with the emergence of technology and rise of globalisation bringing new opportunities as well as new challenges to how data is protected. Looking slightly ahead with the emergence of the next generation of technologies, such as cloud computing, virtualisation, and the development of more personalised online services, it is only likely that additional challenges for the protection of data online will be seen. The rise in cloud computing and virtualisation will increasingly see information processed in remote locations, shared infrastructures and stored on a number of different platforms, applications, networks and servers. As a result data will increasingly be accessible from a variety of locations through web facing devices and platforms resulting in the very way information is stored and accessed changing. The integrity, confidentiality, availability and security of data as it moves away from an organisations protected infrastructure will therefore become even more vital. This evolution in data centre technologies will also enable the delivery of more personalised goods and services online, such as personalized marketing and software as a service.

Therefore gaining and maintaining the trust and confidence of individuals that their information is protected, secured (and assured that it is being used appropriately for the reasons for which it was collected) will be a challenge that must be faced and addressed not only by organisations but also the current legal and regulatory framework.

However, recent high profile incidents of data loss and individuals concerns over the protection of personal information, both in the offline and online worlds, have highlighted the importance that citizens are placing on the role of data protection rules and law. A survey conducted by Symantec in the UK following a high level data breach incident showed that 75 % of people had concerns about how much information companies held about them, whether online or offline and 46% felt that the legislation in place to keep individuals informed about the disclosure or loss of their personal data was inadequate. The rise in data loss incidents has resulted in data protection issues become front page news across Europe and around the world. Not only can this be seen to have raised greater awareness of data protection issues by citizens it also helped to raise greater awareness of the risks and threats information face in the online environment with data becoming a valuable commodity and asset to cyber criminals.

According to Symantec's Internet Security Threat Report published in April 2009 it is data, rather than computer servers themselves, which is now a key target for cyber criminals and online attackers due to the value attached to information that can then be used in phishing, spam and identity theft related attacks. According to the report roughly 90% of the top 50 malware was designed to steal information. As the online threat environment continues to evolve organisations are understanding the importance of having appropriate and effective data protection and privacy policies and procedures in place that ensure the security of their customers information. However, it is equally important that an effective and appropriate regulatory and legal framework is in place that can assist organisations to fully protect personal data.

2. In your views, the current legal framework meets these challenges?

The legal framework established by the Data Protection Directive, with its broad principle based approach, use of common concepts, definitions and appropriate exceptions has enabled the application of 95/46 to remain flexible, technological neutral and adaptable by Member States since 1995. In fact given the growth of e-commerce, online engagement and the web 2.0 world that has emerged since 1995, it can be argued that the principles have provided an effective framework that has enabled the development of effective online business models and increased social interaction online. The principle based approach therefore continues to be supported by Symantec and any review of 95/46 should not attempt to re-engineer the eight guiding principles of the Directive. The current eight principles have not only proven to be effective in enabling data to become the currency of the digital age but can also be seen to have influenced the development of data protection laws in other countries around the world.

Over the past fourteen years the size and shape of the European Union has certainly changed. However a fundamental founding principle of the European Union has remained the creation and development of a single internal market. The harmonisation of European laws has been a fundamental step to achieving this objective. It is argued that the Data Protection Directive has shown how a common legal framework approach can be developed and applied across all European Member States. It has provided a constant framework upon which Member States, both old and new, can develop laws for the protection of data based on common legal definitions and data protection language.

Given that the threats to data held by organisations have increased dramatically since 1995 data protection legislation and regulations has been vital for providing organisations with guidance on the appropriate technical and operational measures that data controllers should use to protect and secure the integrity of online network and services. The legislative principles outlined in the Directive (Article 17) focussing on the need to ensure appropriate technical and organisational measures in place to protect the security of personal data are supported by Symantec and have proved effective as they are technological neutral and appropriate to the risks being faced by organisations. However, it is suggested that this Article was developed in an age where networked computing was still in its infancy and the realities of today's networked, multiple platform world was not envisaged. With the move away from closed, nationally protected computer networks to a more borderless, open, accessible and networked environment, safeguarding information held in electronic networks and systems from possible attack or disruption has

become a crucial component of critical infrastructure protection. To do so however, requires a change in policy approach to ensure that issues that now impact, and affect, more than one European Member States are addressed effectively. The security, integrity and availability of network and services and the information that flow across these networks is therefore vital to protect the resilience and robustness of EU information and communications networks.

With the rise in online business models and the increased sharing of European citizens personal data outside the boundaries of the Union, the requirements in the Directive related to cross border transfers of data (Article 25) have been effective in enabling and managing the increased internationalization of information. In particular the need to ensure that the protections in place in the final destination country are adequate given the nature, purpose and duration of the processing involved before any data transfers are conducted. This requirement is of course vital and should be retained in any review of the Directive. However, it is suggested that a review should also consider what additional protection could be further enhanced in Articles 25 and 26 given the internationalization of information and current online threat environment. For example it is suggested that before a non EU countries protections are even assessed for their adequacy the actual risks to the data in the country to which it is being transferred should be fully assessed. Data is seen as a key target for online attackers and cyber criminals and therefore will always be at risk. Therefore it is suggested that only once the risks to the data are fully identified and assessed can the level, or “adequacy”, of the protections put in place to protect the data transferred be reviewed and assessed.

The Directive's principle based approach can also be seen to have created a legal and regulatory framework that has facilitated the integration of data protection regulatory requirements into organisations every-day processes, policies and procedures. The creation, profile and take-up of internationally recognized industry based standards and specifications, such as BSI 10012:2009 and ISO 27002:2005, and the development of industry best practice methodologies that provide a framework around which organisations can build programs to comply with the Directive, is a sign of how ingrained the Directive's requirements have become to businesses management and security of data. It is suggested that a more prescriptive approach to the Directive's requirements may not have enabled the integration of data protection standards into the day to day operations of businesses or encouraged the development of innovative industry approaches to finding effective and efficient means of complying with the Directive's requirements.

While the EU has certainly grown and technology evolved in the years since the Directive was introduced a key constant has been the presence of Member States Data Protection supervisory authorities established by Article 28 of the Directive. Data Protection authorities play an important role in providing advice, guidance and assistance to organisations on how to ensure compliance with the Directive's requirement. Their independence status and structure is a key factor in their ability to use the powers of investigation and intervention that enable them to ensure compliance with the Directive as well as local laws and more widely engage with industry. However, given data's role as the currency of the digital age it is suggested that the demands on data protection authorities time and expertise will also increase. To ensure authorities can continue to be effective it will be important that they have sufficient funding and resources to be able to address data protection issues as and when they arise. Therefore while a review should maintain the independent status of the data protection supervisory authorities it should consider the funding and resource needs and requirements of authorities and how these could be met to ensure they can continue to be an effective independent enforcer of data protection laws across Europe.

While data has become more fluid with citizens increasingly sharing their personal information to gain access to goods and services, particularly online, at heart of the framework has remained the principle and requirement around notification and consent. These principles are fundamental elements and core principle of data protection legal framework, and remain relevant today and should be maintained. The importance placed on the principle of consent can not only be seen in the emergence and take up of privacy policies by companies (as a means of notification and gaining consent from individuals for data processing) but also individuals awareness of data protection issues as seen by the use of data subject access requests.

The Directive's introduction of a data subject's right to access has become an important tool for empowering individuals to have a means by which to raise questions about how their information is being used and enable greater transparency and understanding about how their information is being processed and stored by organisations. The data subject access request provision has become a well

known element of the Data Protection legal framework in many Member States such as the UK. The fact that consumers are aware of its existence is an example of how the Directive has been effective in providing a legal framework that recognises the rights of European citizens as the owners of their data.

However, now in 2009 and in light of recent incidents of data loss and individuals increased concerns over the protection and privacy of their data the review is an opportunity to consider how the regulatory framework could be further enhanced to ensure data protection remains transparent and relevant to individuals and the legal framework in place continues to work more effectively. For example further discussion is needed around what happens if data is lost or stolen and the need for increased legal clarity and certainty as to what should be considered personal data to ensure all data is secure and protected as necessary. These are issues outlined in further detail below.

3. What future action would be needed to address the identified challenges?

Symantec believe a review of Directive 95/46 is an opportunity to facilitate discussion on the continued relevance, applicability and appropriateness of the Directive in today's technological driven world given the challenges outlined above. The following outlines in more specific detail aspects of the Directive that should be considered for amendment in any review. These include:

- Current definition of personal data
- Introduction of a European wide data breach notification requirement
- Role of risk management based requirements for data security measures
- Appropriateness of the "adequacy" principle for non EU data transfers
- The importance of the consent principle
- Role of PETs
- Internal market issues and the current burden of multi-registration requirements for data controllers across all Member States

Current definition of personal data

The Directive's principle based approach continues to be supported by Symantec and any review of 95/46 should not attempt to re-engineer the eight guiding principles of the Directive. Clearly there are dangers associated with taking a more prescriptive approach to data protection legislation in light of the fact that information technology rapidly out steps regulatory change; legislation should not try to run behind, or even ahead, of technology. However, having in place extremely broad definitions within legislation may also lead to a lack of legal certainty and as a result unintentional misinterpretation and lack of compliance with legal requirements in place. Legislation and regulations based on principles, such as 95/46, provide much needed direction and guidance to organisations on how to comply with legal requirements. Therefore Symantec believe it is important that any changes to data protection laws in Europe should not undermine the inherent value in the principles-based approach. Rather the review is an opportunity to renew the premise that legal direction can and should be sought from the application of these fundamental principles which remain relevant today as they did in 1998.

However, it is suggested that the review is an opportunity to consider how the definitions used in the guiding principles are being interpreted and how they might be improved in order to reduce any possibility of misinterpretation or non-compliance and address emerging challenges. To ensure the Directive continues to remain appropriate and effective in today's information driven age Symantec believes there is a need to review how the current definition of personal data is being interpreted and to what extent it may benefit from further clarification and amendment in light of the technological changes and challenges outlines above.

Overall Symantec remains supportive of the Directive's definition of personal data as "any information relating to an identified or identifiable natural person"¹ either directly or indirectly. It is a key foundation

¹ Article 2 Definitions (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

upon which the data protection laws principles, requirements and responsibilities are based and should not be changed. However, it must be recognised that this broadly defined principle now operates in an age where information that could identify an individual is diversely located. For example data may be processed by a number of different organisations in various locations and across different technological platforms, systems and even devices. As a result it is becoming less clear about which information could in fact be directly linked to an individual, and therefore should be considered personal data, or how close to an individual's information needs to be able to provide a link either directly or indirectly. For organisations it is becoming less clear who may have which 'bits' of information or pieces of the information puzzle that can identify an individual.

It is clear that the sheer volume of all categories of data being collected and stored by organisations is increasing and as a result information may be bundled together in a way that could identify an individual. However, it is also very possible that there may be legitimate reasons and circumstances where private sector organisations may process information relating to an individual that is not bundled with other data and as a result cannot simply be classified as personal data. Such a circumstance is in relation to Internet Protocol (IP) Addresses. A number of recent diverging court judgments in a number of Member States has raised questions over the role of IP addresses and whether they should, or should not, be considered as personal data and therefore able to identify an individual. However, it should be remembered that while an IP address can be used to detect and block online attacks they are inherently unreliable as an identifier given that IP addresses can be easily faked or even hijacked.

Given public concerns over the security and privacy of their personal information when shared, processed and stored by providers of online goods and services, it is perhaps rather tempting to simply classify all data collected as personal data. However, in the case of an IP address only if an IP address is directly linked with an individual's personal data, such as via subscriber information held by an ISP and only accessible when requested by law enforcers using a warrant, can it provide a snapshot of the usage of a particular system at a particular moment in time.

The recent steps taken in the review of the e-Privacy Directive (2002/58) to address similar interpretation issues related to the role of traffic data have been welcomed by Symantec. However, it is felt that issues around the interpretation of the definition of personal data also need to be considered in a review of 95/46. If not addressed it could lead to a lack of legal clarity and certainty for many organisations collecting and holding data as to whether it can or cannot be considered personal data. It is suggested that a lack of uncertainty could lead to the definition of personal data being open to misinterpretation and therefore unfortunately perhaps also a justification for non-compliance with (or abuse of) the Directive itself. Also uncertainty around the definition of what is personal information, particularly in the online world, could become a challenge and barrier to the future development of information society services in Europe and therefore impact the growth of Europe's knowledge society and competitiveness in the digital global marketplace.

Symantec feels this issue warrant further discussion and consideration in the review of 95/46 in order to address, and find a workable solution to the continued legal uncertainty and lack of clarity on how to define personal data in the information age and when such elements of data, such as IP addresses, should and should not be considered personal data. In particular the review of 95/46 provides an opportunity for Europe to assess and consider how close to an individual information needs to be to provide a direct link to this person, and when data may not provide this link how such data should still be protected within the legal framework. The review would also provide an opportunity for Europe to provider leadership in debating this vital issue that is also being considered by other around the world.

Need for European Data Breach Notification Requirement

Symantec welcomed the recent moves taken by the European Parliament, Council and Commission to introduce a data breach notification law as part of the review of the Telecommunications Regulatory Framework. The approach taken in developing an appropriate data breach notification text introduced in Article 4 of the Privacy and Electronic Communications Directive (2002/58/EC) is supported as an important move in the right direction to increase levels of data security and also help raise awareness, and reassurance, amongst citizens across Europe of how their personal data is being secured and protected by telecommunication sector operators. However, given recent incidents of data loss in other key sectors, such as finance and retail, Symantec believe now is the time for organisation and companies in all sectors, public and private, that are processing and storing

individuals personal data electronically to be required to comply with a data breach notification law. This could be achieved by the introduction of a breach notification requirement in Article 17 (Security of processing) of Directive 95/46 on the basis of the language introduced in Article 4 of 2002/58.

That is not to say that the current European Data Protection law (Directive 95/46) is not effective or failing to protect individuals' data; data protection law protects the lifecycle of data from its collection, processing to its storage. However, it is suggested that the Directive 95/46 does not explicitly address circumstances where data is actually lost or stolen and the responsibilities that attach to such loss or theft. The general seventh principle of the Directive requires appropriate measures to be taken to prevent unauthorised processing of data. However, there is no *explicit* legal obligation or requirement to provide notification of a data breach and it is therefore suggested that currently the Data Protection Principles are open to interpretation and could be clarified further by the introduction of a explicit notification requirement in Article 17.

However it is recognized that a breach notification is not a panacea. While breach notification has been a powerful tool in countries such as the US in helping to enforce accountability, there is also a danger of over-reliance on breach notification which can lead to 'breach exhaustion' where consumers now routinely ignore notifications. Therefore any European sector wider breach notification must be balanced and appropriate and mirror the approach that has been taken in the review of the ePrivacy Directive 2002/58.

While Symantec feel that any review of 95/46 must consider the introduction of a sector wide data breach notification requirement, it is understood that a full in-depth review of the Directive could be a lengthy process that will require considerable time. However, as the Symantec Internet Security Threat Report indicates the risks and threats to information are increasing and the incidents of data loss affecting various sectors. Therefore Symantec believes that the introduction of a data breach notification requirement into European law for all sectors is a key priority and warrants the introduction of a separate Data Security Directive to introduce a breach requirement as a matter of urgency. It is suggested that a Data Security Directive could be introduced in a short period of time by simply extending the breach requirement introduced by Directive 2002/58 to all sectors. If this can be achieved it is also suggested that a Data Security Directive could also provide an opportunity to extend the security requirements, also introduced in 2002/58, for all companies to have in place a security policy which is regularly audited and take a risk assessment and management approach to data privacy and security.

Enhancing security of data processing

If the introduction of a Data Security Directive is not considered possible at this time, Symantec believe that a review of 95/46 should consider how Article 17 could be further enhanced by the introduction of the security measures introduced into 2002/58.

A key concept for ensuring the security of data being processed, outlined in Article 17, is the need to ensure the level of security introduced is "appropriate to the risks" involved. Article 17 therefore recognises the need to take a risk management approach to implementing appropriate security to protect data. However, it is argued that the Article does not go further to require a risk assessment and management approach be taken or a security policy to be in place and audited to secure data being processed. These requirements have for example recently been introduced in the review of the ePrivacy Directive (2002/58) to increase the security requirements on telecom providers. It is argued that such security requirements should not solely rest with organisations in one particular sector and should be required across all sectors. Article 17 could be enhanced by including additional security requirements mirroring those introduced into 2002/58 the requirements will complement the Directive's requirements relating to implementing measures "appropriate to the risks" facing data and introduce more specific requirements for risks to be considered and a security policy to be in place and regularly audited. These changes could be achieved simply by introducing into Article 17 the measures recently agreed in the review of Article 4 of Directive 2002/58.

Cross-Border data transfer

Symantec believe it is important to assess the current effectiveness of the adequacy based principle outlined in Article 25 and whether changes may need to be made in this area particularly in light of the increased globalization of data since 1995. The recently published UK ICO – RAND report on the

EU Data Protection Directive considered the rules relating to international data transfers, and the need to ensure the appropriateness of the adequacy principle. This is an area that Symantec believes does warrant review given the adequacy principle's vital role in ensuring data is only transferred to non EU countries that have an adequate level of security and privacy to protect data being shared. The adequacy principle remains sound. However it is suggested that the protection given to European data could be further enhanced by introducing into Article 26 an explicit security requirement for a risk assessment to be taken before the adequacy principle is considered and applied.

While Article 17 does state that the level of security given to data must be "appropriate to the risks represented" by that processing Symantec feels more could be included in the text of Article 17 to embed a risk based approach to data being transferred outside the EU. A risk based approach to assessing the security needs of electronic data has recently been introduced in the review of 2002/58. If such an approach is to be taken for data processing within Europe, Symantec believes it would also be wholly appropriate for this approach to be mirrored in Article 26 when the question of cross border data transfers is considered. It is suggested that a new paragraph is included to introduce an explicit requirement for a risk assessment and management approach to be required as the first step and basis for consideration. This principle approach should include a requirement to assess the data that is being transferred and the risks to that data in its final location. Only then should the question of whether there is an "adequate level of protection" in that place be considered. Clearly the adequacy of the protection in place for the data can only be assessed when the risks to the data in the country where it will be sent are fully understood. It is suggested that introducing additional security requirements before the adequacy principle is applied could enhance the level of security and protection given to information before it is shared outside the EU. Also introducing this additional step could enhance the role and importance of the adequacy principle in the data protection framework and by doing so encourage organisations to take a risk based approach to information security by explicitly requiring risks are fully considered before data transfers are conducted.

Consent

The continued evolution and maturity of the internet will see the provision of increasingly sophisticated and advanced online goods and services that are personalised based on the information provided by individuals. With this future upon us Symantec believes it is important that the principle of consent remains at the heart of the legal framework following any review. It is suggested that the very action of providing consent ensure the involvement and participation of users in the decision made, particularly online, and transparency between the companies and individuals on how their information will be used. While the principle of consent should not be amended it is suggested that a review of 95/46 could be an opportunity to investigate and assess how the consent mechanisms could be further enhanced so that it remains an integral part of the legal framework. The review would be an opportunity for all stakeholders involved in data protection issues to consider how consent models could act as a means of raising data subject's awareness and trust in the measures organisations are taking to ensure data is protected and secure.

Role of Privacy Enhancing Technologies

Symantec believes the review is an opportunity to discuss the current development and maturity of Privacy Enhancing Technologies and the interaction between PET's and Directive 95/46. Since the Commission's Communication on PET's was published back in 2007, a range of privacy technologies have been developed that could be classes as PET's. While PET's are often seen to be focusing on the economisation of data to ensure privacy, a range of PET's have developed that also play an important role in providing data minimisation, ensuring effective data management and therefore data security. In fact it can be argued that there cannot be data privacy without having in place effective information security. However, it is important that any PET's or security measures that are introduced onto online platforms, networks and systems to address data protection issues are conducted in a way that is transparent, interoperable and also enables programmatic disablement to ensure consumers choice. Therefore it is suggested that the Directive's review is perhaps an opportunity to consider further whether the definitions and notions of PET's continue to be appropriate to the way technology has evolved since the Commission's Communication introduction.

Depending on the findings of any reassessment of what should be considered a PET an issue that could be considered is the way in which PET's interacts with the Directive and whether there is a need for specific guidelines to be developed for Member States on the role of PET's and how they interact with 95/46. However, we feel it is important that the Directive retains the technological neutral approach that has proven effective and not seek to introduce specific requirements within the Directive relating to PET's or Privacy by Design. If the review of 95/46 were to introduce a specific technical specification for PET's or Privacy by design, to be included in the design and inclusion of services and products this could not only impact the future interoperability of systems across Europe but also create a single point of failure in online systems and networks. By mandating a common technological approach or solution that is shared across all European networked systems and infrastructure that process and share data, this increases the likelihood that a single threat or risk to one system could be shared by all those that are interconnected. Therefore this discussion should focus on finding ways to promote the use of PET's and encourage the market's development of PET's as a "technical measure" that can enhance the privacy of data. For example, identifying best practices that could be promoted by such organisations as ENISA particularly in their work with SMEs to encourage the take up and use of PETs.

Internal Market Issues

The harmonisation of European law is a key tool for enabling companies to operate across European geographical borders without having to contend with the complication of complying with multiple different legal systems and regulatory requirements. The principle based approach of 95/46 supports the development of greater European legal harmonisation and is therefore supported. However, it is suggested that the requirements for data controllers and sometimes even data processors to register with each Member State's supervisory authorities responsible for data protection enforcement the purposes and type of data being processed before carrying out data processing should be reviewed in light of the impact this multiple registration requirement may be having on data controllers and/or processors. The question is whether this current approach is conducive to the principle of legal harmonisation and even the further development of the internal market. This multiple compliance requirement has a significant administrative and logistical and therefore financial impact on organisations particularly SMEs. It would also appear to be a demand that is at odds with the harmonisation principle in the area of data protection and also the better regulation agenda being supported by many Member States such as the UK. A review of 95/46 should consider the administrative, financial and operational impact the registration requirements in Article 18 and 21 are having on organisations across Europe and explore alternative registration options that could not only ensure that the important requirement of registration is maintained but in a way that is more efficient, cost effective and harmonised. For example it is suggested that consideration could be given to the use of the country of origin principle from the eCommerce Directive within 95/46 that would see organisations only being required to register once with the Supervisory Authority within the country the companies operations are registered. Therefore any issues that may arise from the processing of data, by the data controller, would be addressed by the Supervisory Authority within the Member State the data controller is based regardless of where the individual whose data is being processed resides. However it is recognised that for this approach to be workable Member States would need to recognise registrations made in other European Member State

In addition to these suggested approaches the Directive's review should also consider areas where there may be a need to strengthen existing measures, or formally recognise and support methods used by companies to comply with the Directive. For example the use of Model Clause Data Transfer Agreements and Binding Corporate Rules (BCR).

The model clause approach is a primary mechanism many companies use to achieve compliance with 95/46 and should be supported further by the Directive. However, a review of the Directive is an opportunity to discuss and consider further the appropriateness and current effectiveness of the current Model Clause agreements given the growth of global outsourcing since 1995 and the increasingly complex multi-tiered sub contracting business models that have emerged and are currently in place across and beyond the EU.

The recent steps that have been made to allow BCR to become an effective method for organisations to meet compliance objectives, through the use of sponsoring states to simplify the approval of BCR arrangements have been welcomed. However, the 95/46 review should further consider and discuss

ways in which the processes and procedures for attaining BCR status can be simplified in order to encourage and permit more multi-national organizations to comply with and obtain BCR status.