The EU Data Protection Directive revised: New challenges and perspectives

By Maria Giannakaki
Attorney-at-Law, D.E.A.
giannakaki.m@dsa.gr

I. Introduction

Our society undergoes fundamental changes due to the rapid technological developments and globalization that have given rise to the processing of data on a worldwide scale and an increase in international cross-border data transfers. The expansion of social networking services (SNS) and the growing demand for cloud based services (IaaS, Paas, SaaS) trigger new perspectives, but also new practical data protection challenges.

Although it is accepted that widely applauded principles of the EU Data Protection Directive 95/46/EC for the protection of personal data still remain valid, it is equally acknowledged that the existing EU legal framework needs to be revised in order to cope with the evolutions.

To that end on November 4, 2010 the European Commission released a Communication proposing 'a comprehensive approach on personal data protection in the European Union" with a view to amend the EU Data Protection Directive 95/46/EC ("the EU Directive").[1] The Communication is the result of the review of the current legal framework, which started with a high-level conference in Brussels in May 2009 and was followed by a public consultation during 2009 and 2010.[2] On February 2011, the Council of the European Union released its conclusions on the Communication and outlines the main axes of the reform.[3]

This paper aims to analyze the data protection challenges under new technological and social developments, examine how the current data protection rules address these issues and identify the possible solutions in light of the current reviewing process of the EU Directive.

II. Challenges: Technical and social developments

II.1. Utility computing – The 'cloud'

In recent years, cloud computing has emerged as one of the fastest-growing segments of the information technology industry. According to the European Network and Information Security Agency ('ENISA'), the worldwide forecast for cloud services in 2013 amounts to USD 44.2bn, with the European Market expected to go from € 971 in 2008 to € 6005 in 2013.[4]

Cloud computing *"is an on-demand service model for IT provision, often based on visualization and distributed computing technologies*"[5]. It is an internet-based model of computing enabling the provision of various services upon demand, such as

Infrastructure "IaaS" (e.g. compute power, storage, servers and related tools, such as Windows Live Skydrive and Rackspace Cloud), Software "SaaS" (e.g. software applications deployed as a hosted service and accessed over the internet via a standard web browser such as Zoho.com, Google docs) and/or Platform "PaaS" (e.g. operating systems and associated services over the Internet without downloads or installation such as Google App Engine)[6]. For the provision of such services, Cloud Service Providers ("CSP") are based on *"a networked collection of servers' storage systems and devices combining software, data and computing power scattered in multiple locations across the network*."[7]

Cloud computing offers several benefits for both users and service providers, such as services provided on demand without the need for certain software or hardware at the physical point of access, cost savings, easy access and implementation by small and medium enterprises (SMEs) etc.[8] Arguably, "the cloud" is turning computing into a utility due to the fact that it enables the packaging of computing resources, such as computation, storage and service and makes them available on demand in a way similar to the traditional public utility (such as electricity, water, natural gas or telephone network).[9]

However, due to its ubiquitous and dynamic nature cloud computing also raises serious concerns from a data protection and privacy perspective. In the "cloud" the CSPs' servers are located in several jurisdictions, data is processed and 'duplicated' in a variety of locations around the world and transferred from one location to another and infrastructure used to store and process a customer's data is shared with other customers. Data processing "in the cloud" involves outsourcing partial control over the storage, processing and transmission of such data to a CPS due to the fact that the CPS determines the location of data, the service and the security standards.

On 03.02.2011 the Danish Data Protection Authority issued a Resolution (0138-52-2010), rejecting the Municipality of Odense's planned use of Google's Cloud Computing services within schools over cloud privacy risks.[10] Last year the German Data Protection Authority issued a Framework Paper and an Opinion addressing the various legal concerns regarding personal data protection and data transfer in the cloud, with the aim to impose tougher restrictions and requirements to cloud computing and other outsourcing arrangements involving personal data.[11]

Cloud computing triggers several legal issues from a data protection point of view which can be summarized as following:

1.1. Applicable law in the cloud: Territoriality v. country of origin principle

Under the EU Data Protection Directive (art. 4), *"each member state shall apply the national provisions it adopts pursuant this Directive to the processing of personal data where:* ***a.*** *the processing is carried out* ***in the context of the activities*** *of* ***an establishment*** *of the controller on the Territory of the Member State or in a place where its national law applies by virtue of international public law or* ***b.*** *the controller is not established on Community territory and for purposes of processing personal data* ***makes use of equipment,*** *automated or otherwise, situated on the territory of the said member unless such equipment is used only for purposes of transit through the territory of the community."*

Under the current provisions of the Directive, the starting point of the applicability criteria is the place of establishment of the organization making decisions about the use of data or the use of equipment situated in the territory. Preamble 19 of the Directive clarifies that *"establishment on the territory of a Member State implies the* ***effective and real exercise of activity through stable arrangements*** *and when a single controller is established on the territory of several member states, particularly* ***by means of subsidiaries****, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities".*

"In the cloud" the physical location and the use of means are no longer suitable connecting factors, as data effortlessly flows around the globe, ignoring boundaries and territories, and replicas of users' data are kept in several multiple data centers located at random places and jurisdictions. On top of that, cloud computing services usually involve a multitude of providers, who may process data by determining both the purposes and the means of data processing or may process data on the instructions of their client.

When applying the territoriality principle in cloud computing services, determining which cloud provider is subject to EU data protection rules for what data processing can prove to be a very difficult task. If a CSP is established in the EU and/or uses equipment in the EU, he will be subject to the EU data protection law. However, if he is not established in the EU and/or does not use equipment in the EU, he would not be subject to the European law, even if European citizens' data are processed through cloud computing services.

1.2. Role distribution in the cloud: Data controller v. data processor

The question of applicable law is directly related to the entity which will be qualified as a *"data controller"*. Under article 1 par d and e of the EU Directive the "controller" is the person who alone or jointly with others determines both the *"purposes"* and *"means"* of processing, while the *"data processor"* is the person who processes personal data *"on behalf of the controller"*. The controller is primarily responsible for the compliance with data protection obligations and will also be held liable in case of breach.

With respect to cloud computing, the identification of the data controller can prove to be a very difficult task depending on the type of the cloud computing that is used and the technical set-up of the system. A CPS usually processes clients' personal data "on their instructions" and for the purposes that they have determined. However, at the same time the CPS makes decisions at its sole discretion about the "means of data processing" regarding the location of the data, the service levels, security and the related technical and organizational measures.

Given that the concepts of the data controller and data processor are not clear[12] it would be rather difficult to identify on a case-by-case basis who is the data controller. It is also quite possible that the basic decision on who is responsible for data protection compliance would be contested. It is likely that CPS will consider

themselves to be data processors in order to avoid step in the shoes of the data controller and bear the burden to comply with data protection obligations.

Consequently, the customers, who are very unlikely to know if and when their data are moved, how they are stored, who has access to them and which security measures have been put in place, will end up to be solely responsible for data protection compliance, except maybe from cases like platform as a service where a user does not have any control over the means used to process data or if the CPS analyses users' personal data for the purposes of behavioral advertising.

1.3. Purpose of processing in the cloud: business v. purely personal purposes

There is a tendency to offer cloud computing services to individuals as end users, such as storage of pictures, calendars, typically the type of information one should keep at home and use for personal purposes. However, article 3 of the EU Directive excludes from its scope of application data processing carried out *"by natural persons in the course of a purely personal or household activity* (the *"house hold exemption"*).

Therefore, due to the personal – household nature of information uploaded to the cloud, processing activities that are carried out on behalf of the individuals involved may not fall under the scope of the EU Directive.

1.4. Transfers in the cloud: Jurisdictional approach v. international standards

Cloud computing entails the continuous transfer of personal data. The EU Directive prohibits transfers of personal data outside EU/EEA and a limited number of "third countries" considered by the European Commission as providing *"adequate safeguards"*, based on the presumption that these countries do not always protect personal data sufficiently, unless the CPS provides adequate safeguards for such protection.

Although in theory a variety of possible legal bases for adequate safeguards exists, in the cloud context it is very difficult to implement. A business most likely would rely on data subjects' consent, the *"balance of interests"* test or contract fulfillment.

Obtaining consent inevitably would be burdensome and in any case, raises significant legal issues in Europe, for the reason that the CPS will have to prove that such consent has been freely given and that it is specific, informed and freely revocable. With regard to the "balance of interests test", it would be rather difficult for CSP to apply this test in an international environment, due to its vague and open-ended nature, as well as in the different approaches by each Member State. A third option would be to use the EU model clauses or Binding Corporate Rules, however, given the onerous obligations they entail and the fact that they are designed for multinational companies and do not always work well in a multi-tiered vendors relationship, this option may become problematic too.

II.2. Social computing - Web 2.0

Cloud computing is an innovation in the technical way services are provided. However, nowadays there is also a significant social evolution in the way the Web is used to such extend that many speak about the creation of a new version of World Wide Web: Web 2.0.[13] Arguably, Web 2.0. presents a second generation of web-based communities, applications and hosted services that facilitate participatory information sharing, interaction and collaboration on the World Wide Web. Examples of Web 2.0 include Social Networking Sites "SNS" (such as Facebook, Myspace, Twitter, Linkedin), blogs, video sharing sites, hosted services, web applications and mash-ups.

2.1. Web 2.0 characteristics

Web 2.0 allows users to use "Web as a Platform" in order to create and distribute their own User Generated Content ("UGC"), promotes creativity, collaboration and sharing through mass social networking channels. Furthermore, it facilitates users to express themselves, engage in social and political debates, access and participate in economic, cultural and administrative activities, contribute to the production of knowledge and eventually construct their public profile. Social networking providers (SNP) serve as a tool enabling users to create and exchange content and communication and eventually promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom of expression.

However, the ubiquitous character of information in the Web 2.0 environment poses new challenges to the application and enforcement of data protection principles. Data from different locations and sources are collected, visualized and aggregated by Search Engines, Social Network Aggregators (Spokeo, Pipl)[14] and Mass-ups (Poplfly)[15] in applications that combine different types of information such as geolocalization data, photos, audio and other information and make them available into a single view.

Web 2.0 increases the accessibility to any kind of information related to individuals regardless if it refers to his private, public or professional life and makes it accessible to any internet user who is interested to perform a research about a persons' virtual identity: human-resources professionals report that their companies require them to do on line research image tagging by third parties, many SNS and other providers of "free" cloud computing services (such as webmail) seize the opportunity to monetize users' information by including targeted advertisements in their offerings. Soon Web 2.0 will be used as a platform by which people will be rated, assessed and scored not only on their creditworthiness, but also on their reputation and trustworthiness as good parents, dates, employees, insurance risks etc.

In addition to the above, information is copied, tagged, reposted and remains in search engines, aggregators, mass-ups and internet archives for an indefinite period. Technology enables users to retrieve in a matter of seconds' information which would otherwise be forgotten – and 'forgiven'. According to ENISA, Internet in the Web 2.0 era has the "Hotel California impact" on individuals: *"They can check out any time they like but they can never leave"*[16].

2.2. Data subjects' rights under the current legal framework

The aforementioned characteristics of social computing, result to a loss of control over individuals own data, due to the fact that it is practically impossible to know what data are being collected, how they are processed on what context they are used and for what purpose and if they are secure. Information is '*alienated'* from the individual and the context in which it has been initially disclosed.[17]

Under the current EU data protection framework, the constitutional right to informational self-determination[18] warrants the capacity of individuals to determine in principle the disclosure and use of their personal data and decide what information about themselves should be communicated and under what circumstances. In addition to that, the EU data protection Directive provides for data subjects' right to access and/or rectify their personal data, withdraw their consent for data collection and processing or delete them.

Furthermore data controllers bear the obligation to keep data collected for a specific retention period which is related to the scope of their processing and in any case they should keep data no longer than necessary. Given that this specific period lapses, they should delete them in order to satisfy data subjects need to "be forgotten'.

However, Web 2.0 platforms make the application and enforcement of these rights extremely difficult. In an attempt to strengthen data subjects' rights and help them ensure control over their data, the *"right to be forgotten"* is proposed to be inserted in the revised EU Directive.

III. Perspectives – Key issues for amendment

The aforementioned challenges of the new technological and social developments are addressed among others in the ongoing procedure of amendment of the EU Directive.

III.1. International dimension of data protection

1.1. Applicable law

Under the current provisions of the EU Directive, it is not always clear to both data controllers and data protection supervisory authorities which member state is responsible and which law is applicable when several member states are concerned. It is therefore commonly agreed that there is a need to enhance legal certainty and avoid potential conflicts between overlapping data protection laws. More specifically, the Council concluded that "*the new legal framework should clearly regulate the issue of applicable law within the EU in such a way so as to allow data subjects to effectively exercise their rights and to provide legal certainty to data controllers in cross-border activities."*

To that end, it seems that all parties[19] agree that privacy standards for EU citizens should apply independently of the area of the world in which their data is being processed and that the national privacy authorities should be endowed with powers to investigate and engage in legal proceedings against non-EU data controllers whose

services target EU consumers, such as US based social network companies which have millions of active users in Europe or cookies from non-EU sites.
More specifically, the criteria for determining applicable law should change from establishment and equipment to citizenship or residency. The country of origin principle is presented as a better, clearer and unambiguous rule on applicable law, which shall enable each Member State's law to apply to the state citizens or residents in the same way as for example the US Federal Trade Commission standards apply with respect to enforcement of the Children's Online Privacy Protection Act, in case that US children are targeted by a service provider.

However, it has been identified[20] that harmonization or at least approximation at a high level between the laws of the member states is an essential prerequisite in order to avoid "forum shopping".

The concept of *"targeted individuals"* or the *"service orientated approach"* is also followed by the EU Regulation 593/2008 on the law applicable to contractual obligations (Rome I), which provides that the absence of a valid choice of law a consumer contract *"shall be governed by the law of the country where the consumer has his habitual residence provided that the professional: a. pursues his commercial or professional activities in the country where the consumer has his habitual residence or b. by any means,* ***directs*** *such activities to the country or to several countries including that country"*. Further guidance with regard to the criteria of *"directed activity"* can also be found in Recital 24 of Rome I." [21]

1.2. Harmonization within the EU/EEA countries

The Council recognizes that the most important element of a well-harmonized approach in Member States is a new legal framework providing for a higher level of harmonization than the current one, without specifying the legal instrument by which this harmonization could be achieved.

There are various suggestions as to how this purpose of harmonization can be achieved: The European Data Protection Supervisor advocated for a regulation rather than a Directive for the reason that if the new legislation takes on the form of a Regulation, it would be directly applicable to all member states under the EU law, without the need for a separate implementation into national law, as would be the case for a "Directive" and that would considerably facilitate the global transfer of data outside the EEA. [22]

Regardless the above proposal, it is widely accepted that there will be no need to amend the Directive or to insert a Regulation but give the power to the WP29 to carry out more in-depth, surveys of national laws and practice with the view to formulate best practices and suggested interpretations.[23]

1.3. Simplification of International Data Transfers

With regard to the International Data Transfers, the challenge would be to find a model that achieves in practice without imposing disproportionate burdens on organisations, economic development or innovation of multinational companies in particular.

To that end, the Commission intents to improve and streamline the current procedures for international data transfers, including legal binding instruments and BCRs in order to ensure a more uniform and coherent EU approach vis-à-vis third countries and international organisations.

This goal can be achieved by a greater recognition of adequacy of non EU/EEA companies, as well as a review of the BCRs as a legal basis for data transfer. In addition to the above, the Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data presented to the 31st Conference of Data Protection and Privacy Commissioners would also provide valuable assistance.[24]

III.2. Individuals rights

2.1. Right to be forgotten and data portability

The Commission in its Communication announced that it wishes to find ways to clarify the *"right to be forgotten",* the right of individuals to have their data deleted when they are no longer needed for legitimate purposes especially in cases that processing is based on the person's consent which is withdrawn or when the storage period has expired. The right to be forgotten will complement the existing rights of data subjects by ensuring data portability: the explicit right for an individual to withdraw his/her data.

The Council encouraged the Commission to explore the introduction of a *"right to be forgotten"* as an innovative legal instrument, even though the exact content of such right and the conditions on which it will be exercised has not been defined yet.

The *"right to be forgotten"* is not a new concept. The right to oblivion (droit a l' oubli) is a right related to data subject's right to withdraw their consent for data processing and have their data deleted[25] [26] and is directly related to the right to informational self-determination.

According to the European Data Protection Supervisor, the *"right to be forgotten"* would ensure the deletion of personal data or the prohibition to further use them without necessary action of the data subject under condition that such data has already been stored for a certain amount of time. To that end, data will be attributed to some sort of expiration date.[27] Furthermore, the EU Commissioner for Justice Fundamental Rights and Citizenship clarified that data subjects and especially consumers will have the right and not the possibility to withdraw their consent to data processing and ask for the deletion of data being held on them, under condition that they prove that the collecting of their data is no longer necessary.

The *"right to be forgotten"* has been strongly criticized and has given rise to serious concerns regarding its achievability in the new technological and social environment, which can be summarized as following:

The exact content and scope of the right has not been clarified yet, obviously due to the fact that it would be rather difficult to determine what kind of records/information will be covered by such right (e.g. what is it to be deleted? the entire record? copies of

records sent to third parties? archived copies?), who will be entitled to such right (when records e.g. are associated with multiple individuals), who will be subject to it and what would be the duties to b;e imposed (e.g. what would be the duty of a blog service in the context of an anonymous speech, where it would be unable to contact the creator of the record to be deleted).

The new powers that the new right actually entails are not clear. The right is implicitly established in the EU Directive, with the principle of data retention and the existing duty to keep data no longer than necessary in relation to the scope of their collection and data subject's rights to access, rectify or delete data.

Such right should be carefully expressed in order to provide for counterbalancing exemptions where there is a need to preserve data irrespective of the individuals' wishes e.g. for journalistic, literary and artistic purposes, freedom of expression, freedom of press, freedom of society to record history etc. Striking the appropriate balance between an individual's "*right to be forgotten"* and other individual or societal interests such as the freedom of expression and the freedom of the press would be rather difficult and situations where the deletion is impossible, infeasible or socially harmful should also be addressed under the revised EU Directive.

The *"right to be forgotten"* has raised serious objections due to the fear that such a right may end up as a tool for censorship or the suppression of civil liberties in order to create a digital identity including only good information. There is a fear that it is rather possible that users may invoke libel or defamation in order to justify censorship about things that hurt their reputations.

The application of this right becomes much more complicated when related to the Web 2.0. platform providers, due to the fact that data to be deleted refer to the user's content rather than the platform's traffic data, as it might have been the case with the debate relating to cookies, logs data retention and e-discovery. For example, when data are published on an SNS, they are practically published to the whole Internet. The SNS may be able to offer deletion only in its own environment but not to other environments (such as search engines).
When it comes to search engines, mash-ups or social network aggregators things may become much more complicated with regard to the rights applicability: It is not obvious who will have the right to decide the data deletion in such cases. The SNS provider will be held responsible once the source of information is deleted from its site, to make sure that all reference to such information on the Internet is deleted? How can SNS delete information not included in their sites?

In addition to the practical and technical problems related to the deletion of information appearing in various different platforms on the Internet, there is also the issue related on the criteria on which platform providers will decide that data should be deleted or not. Who will be competent to decide whether the nature of information is defamatory or violates ones privacy? Such control would oppose to the principle that intermediaries do not bear responsibility for the content, unless they are informed.

Two recent decisions of the Spanish Data Protection Authority and the Italian Courts prove that it is not going to be easy to strike the balance between the conflicting rights.

On January 2010, the Spanish Data Protection Authority accused Google of invading personal privacy of users, arguing that the company was in breach of the right to be forgotten. The Authority ordered Google to remove links to more than 80 news articles mentioning people by name saying it violated privacy for the reason that they contained out of date or inaccurate information. Google argued among others that this would be a form of censorship.

On April 2010, the Italian judge found Google criminally liable violating data protection law, in connection with the online posting of a video showing an autistic boy being bullied and insulted. More specifically, Google was found guilty for not taking precautions and not informing uploaders about their liabilities.

The Decision of the Italian Court has been strongly criticized for the reason that the Italian judge failed to conceptualize the role of platform providers in the concept of Web 2.0 and their enabling function with regard to User Generated Content. Establishing provider's liability for UGC would enable them to exercise a preventive and proactive control over the distribution of such content. This role is contrary to the current rules for limiting liability of host providers with regards to the contents published in their websites.[28]

On top of the above, the *"right to be forgotten"* would be rather difficult to apply in an international environment, given the different understandings of the notion of privacy. For example in the US privacy is primarily related to consumers and it does not apply to any information in the public domain.

2.2. Alternatives

It is true that the web as a platform is a field of controversies and conflict of interests and it is questionable if the existing law may effectively address the various issues that arise. However, many think that the existing law deals with this well by permitting data retention as long as necessary and that hyper specific regulation will not work since the cases are simply too varied. Alternatively, the following amendments and measures may be put forward:

Data subjects should be better educated regarding the Web 2.0. so as their consent to be reinforced: "educated" data subjects may acknowledge that the UGC may jeopardize their private life. To that end, the Council supports the efforts of the Commission in drawing up EU standard privacy information notices, including the minimum set of information to be provided to data subjects and acknowledges the major need to increase the data subject's awareness of the implications of sharing his personal data.

Services should be better regulated in order to clarify the existing obligations and liability of the Web 2.0 providers on which ordinary users rely. In particular such hosts should be made to provide default settings for their sites and services and tools that are privacy friendly: If the default settings fail to protect privacy and personal data, the site that chose those settings should carry the primary responsibility for this. This would leave open the possibility of adopting a tort regime under which individuals can be held liable for wrongful or unjustified public disclosure of private information or intrusion over the Internet.[29]

In addition to the above, the existing duty to keep data no longer than necessary, should be further specified and clarified in relation to the specific activities for which data are collected. Data retention policies can be made compulsory and storage periods in data privacy notices can be further specified.

3. Proactive measures and self –co regulation

The EU Directive provides for *"the implementation of appropriate technical and organizational measures by the data controller aiming to protect personal data against accidental loss, alteration, unauthorized disclosure or access".*

However, in practice it is widely accepted that the current notification process and relevant requirements are overly bureaucratic, achieve little real benefit and divert resources of controller and supervisory authorities away from substantial compliance work.

Under the current review of the EU Directive, it is acknowledged that the implementation of proactive measures though out the cycle of data's life can strongly complement law, as following:

3.1. Principle of Accountability

On July 2010, the WP29 adopted an Opinion on the "Principle of Accountability".[30] The WP recommended that a new principle should be introduced, which would require data controllers to put in place appropriate and effective measures to ensure compliance with the principles and obligations set out in the Directive. This principle is not new: article 17 (1) of the Directive requires data controllers to implement measures of both technical and organizational nature. However, these provisions have a limited scope. The Principle of Accountability would explicitly require data controllers not only to comply with the existing principles of the law, but also to put in place pro-active measures ensuring compliance (such as data protection policies, mapping procedures, privacy impact assessments etc), as well as retain adequate evidence in order to be able to demonstrate compliance to authorities upon request.

The WP29 encourages data protection in practice in a more scalable and flexible approach where "*controllers are required to take a strategic, risk based approach when determining effective and appropriate measures based on the nature of the personal information being processed and the risks represented by such processing".*

The suitability of measures to be adopted should be decided on a case-by-case basis in light of the data controller's specific circumstances and of the risks that may result from the data controllers intended data processing rather than requiring data controllers to adopt each and every measure on a predefined list.

Both the Commission and the Council welcomed the principle of accountability which should be explored with a view to diminish the administrative burden on data controllers for instance by simplifying or tailoring adequate notification requirements, including a uniform EU-wide registration form. The principle of accountability is seen as a practical means of ensuring the observance of data protection rules as well as helping data protection authorities in their supervision and enforcement tasks.

3.2. Privacy Impact Assessment

The UK Commissioner in its "Privacy Impact Assessment Handbook" encouraged both government and private entities to undertake assessments in order to assess and identify privacy concerns of a project and address them at an early stage. More specifically, *"Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIA help identify privacy risks, foresee problems and bring forward solutions".* [31]

PIA constitute a form of pre-emptive compliance audit aiming at the identification and evaluation of the potential privacy implications of a system in order to address them at an early stage with a view to control, minimize or even eliminate the risks associated with the private life. It is agreed that PIAs play a vital role in achieving both privacy protection for individuals and risk management to private organizations and government entities, where in some jurisdictions have already become mandatory.[32]

The Council invited the Commission to explore the possibilities of promoting preliminary Impact Assessments however, only in relation to certain categories of data due to the high privacy risks they present, such as biometric data processed especially in the field of police and judicial cooperation in criminal matters.

3.3. "Privacy by Design" Principle

In addition to the early privacy planning with PIA's, the Council invited the Commission to explore the possibility of including a provision on the "privacy by design principle" in the new legal framework related to the whole life-cycle of a system.

The principle of "Privacy by Design" was originally developed by the Ontario Privacy Commissioner according to which *"privacy and data protection are embedded through out the entire life cycle of technologies, from the early stage to their deployment, use and ultimate disposal".* Recently, the 32nd International Conference of Data Protection and Privacy Commissioners issued a Resolution recognizing Privacy By Design as an essential component of fundamental privacy protection. According to the said Resolution, Privacy By Design is based on 7 foundational principals: i. Proactive not reactive, ii. Privacy by Default, iii. Privacy embedded into design, iv. Full functionality, v. Full lifecycle protection, vi. Visibility and transparency, vii. User centric. [33]

"Privacy by Design" also features in the Commission Communication on a "Digital Agenda for Europe – COM(2010) 245[34] by which it is acknowledged that it would empower data subjects to have more control over their personal data, through data minimization, privacy by default (default/initial settings should be protective for users privacy e.g. in social networks privacy by design would require to keep individuals profiles private by default and unavailable to search engines) and implementation of the necessary tools to enable users to limit the unnecessary collection of data and better protect their personal information (e.g. access controls encryption).

3.4. Private Enhancing Technologies (PETs)

The European Commission in its Communication to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), defines PETs as *'a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, without losing the functionality of the Information System".*[35]

PETs can be divided in two categories: PETs for privacy protection (PipeNet - protecting of identity when accessing interactive internet services, privacy technologies for RFID systems (out of tag mechanisms) and PET's for privacy management (such as eBay's Account Guard, Google's Safe Browsing toolbar)[36].

They also include among others automatic anonymization after a certain lapse of time (e.g. anonymous credentials that prove an individual has permission to access specific resources without revealing its identity), encryption tools prevent hacking when the information is transmitted over the Internet (especially encryption for cloud Web services such as Google Docs to store and process data only in an encrypted form ensuring that access is limited to the owners of the data), "cookie-cutters" blocking cookies placed on the user's PC to make it perform certain instructions without being aware of them and Platform for Privacy Preferences (P3P) allowing Internet users to analyze the privacy policies of websites and compare them with the user's preferences as to the information he allows to release.

The Council invited the Commission to favor PETs as it is recognized that PETs are essential tools to ensure effective privacy protections however the challenge would now be to deploy these technologies in mass-market.

3.5. Personal data Breach Notification

The Breach Notification was inserted in the European law with the EU Directive 2009/136/EC (amending the E-Privacy Directive), which imposed notification requirements in case of a personal data breach (a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data) to competent authorities, subscribers and other affected individuals.

The insertion of a Data Breach Notification in the revised EU Directive could also serve as an effective remedy to individuals in order to be made aware of the risks they face when their personal data are compromised. In addition to the above, it could contribute to raise the awareness of data controllers in order to implement stronger security measures to prevent breaches and could also be used as a tool in order to enhance the principle of controllers' accountability.

The Council encouraged the Commission to explore the opportunity in extending data breach notification obligations to sectors other than the telecommunication sector. However, before implementing such obligation the costs to business and EU competitiveness should also be taken into account so as to avoid transforming the obligation to a routine alert for all sorts of security breaches. To that end, all

stakeholders agree that the criteria for this selection should be the specific sectors in danger (such as the financial sector), the categories of events that may need to trigger notification, a risk assessment of the data breach, in order to avoid imposing cumbersome requirements.

3.6. Data Protection Officers and EU Certification Schemes

In addition to the above, the Commission underlined the fact that the current general obligation to notify all data processing operations to the Data Protection Authorities is a rather cumbersome obligation which does not provide, in itself any real added value for the protection of individuals' personal data.

Following, in the attempt to lessen the administrative and regulatory burdens to data controllers, the Council encouraged the Commission to include in its impact assessment an evaluation of the possible appointment of Data Protection Officers and supports the idea of introducing privacy seals (EU certification schemes) and self regulatory initiatives, by "*considering the establishment of a special body or office of the EU/EEA DPAs closely linked to the WP29 and the Commission to deal with the European Privacy Seal, European codes of Conduct and BCRs"*.

The aforementioned schemes may provide comfort to users of certified technologies, however they should ensure that the criteria for granting such certifications are sufficiently technologically neutral and sufficiently flexible to take account of the fast pace of technological evolution.

IV. Conclusion

The Commission will unveil legislative proposals to update the EU data protection legislative framework this summer.

Until now, it seems that the key issues for amendment would include the criteria on the applicable law, the harmonization of the internal market and the facilitation of international transfers. On the contrary, the proposed *"right to be forgotten"* has raised serious concerns by participants and stakeholders.

In addition to the above, even though it has been widely agreed that the roles of the different organizations have expanded far beyond the simple classification of the current EU Directive and are not properly covered by the confusing notions of data controller and data processor, the allocation of their responsibility does not seem to have been properly addressed during the consultation procedure.

On top of the proposed amendments, it is acknowledged that the sole law reform is not sufficient and there is a need for the adoption of preemptive *"quasi legal measures"* by the data controllers. It is acknowledged that it is going to be several years before any revised Data Protection Directive is agreed and in force throughout Europe. Therefore, in the meantime, organizations are encouraged to take the responsibility for their data privacy obligations through the adoption of data privacy compliance programs and in doing so they will hold themselves accountable to the stakeholders for the commitment to good practice.

REFERENCES

[1] European Commission (2010), Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions "A comprehensive approach on personal data protection in the European Union" on line at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf / accessed 01.04.2011

[2] Article 29 Data Protection Working Party (WP29), The Future of Privacy, 01.12.2009 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf accessed 24.03.2011

[3] Councils Conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union (2011) on line at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf/ accessed 02.04.2011

[4] European Network and Information Security Agency (ENISA), 2009, *"Cloud Computing: Benefits, risks and recommendations for information security"*, online at www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing.../fullReport/ accessed 24.03.2011

[5] Id. no 4

[6] Joep Ruiter ans Martijn Warnier (2011), *"Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice",* online at http://homepage.tudelft.nl/68x7e/Papers/spcc10.pdf / accessed 03.04.11

[7] Ann Cavoukian, Information and Privacy Commissioner of Ontario, (2008), *"Privacy in the clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet",* online at http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf / accessed 24.03.2011

[8] Sneha Prabha Chandran and Mridula Angepat *"Cloud computing: Analysing the risks involved in cloud computing environments"* online at http://www.idt.mdh.se/kurser/ct3340/ht10/FinalPapers/16-Sneha_Mridula.pdf / accessed 03.04.11

[9] Nicolas Carr, (2008), *"The Big Switch – Rewiring the world from Edison to Google",* W.W. Norton

[10] The Municipality planned to use Google Apps in order to allow teachers to register among others information about lesson planning and student's educational developments. The Authority expressed concerns about the security of sensitive data, the transfer of data to other countries, deletion of data, use of encryption and whether the data is logged and for how long the log is stored. Decision of the Danish Data Protection Agency on the use of cloud computing services within schools online at http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution /accessed 01.04.11

[11] German Data Protection Authority, (2010) *"Legal Opinion on cloud computing*" online at https://www.datenschutzzentrum.de/cloud-computing &*"Draft Framework Paper on cloud computing"* online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf?__blob=publicationFile#download=1 / accessed 24.03.2011

[12] WP 128, 22.09.2006 and WP 169, 16.02.2010 with regard to the determination of the means of processing and the criterion of the "essential elements of means' online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_el.pdf and http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf / accessed 24.03.2011

[13] O Reilly (2005) "What is Web 2.0" online at http://facweb.cti.depaul.edu/jnowotarski/se425/What%20Is%20Web%202%20point%200.pdf / accessed 01.04.2011

[14] Social Network Aggregators are web sites that aggregate data publicly available from online and offline sources (such as phone directories, social networks, photo albums, market surveys, mailing lists and business sites) and permit username search scan across the web constructing online profiles on real time.

[15] Mash-up is a web-application based technology that uses and combines multiple web sources and creates a new service enabling users to have access to different types of media such as data, video, images, blogs and audio into a single view.

[16]ENISA "Security issues and Recommemdations for Online Social Networks" (2007), online at http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks/ accessed 04.04.2011

[17] Lilian Mitrou "Privacy in Web 2.0" (2010), DiMMEE, 3/2010, page 323

[18] Ruling of the German Constitutional Court defining informational self-determination online at http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm /accessed 23.03.2011.

[19] European Commission, European Council, WP29, the EU Commissioner for Justice, Fundanmental Rights and Citizenship, the European Data Protection Supervisor and participants in the public consultation

[20] European Commission – DG JFS, New Challenges to Data Protection – Final Report http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf / accessed 31.03.2011

[21] Lokke Moerel (2011), "The long arm of the data protection law", International Data Privacy Law, 2011,Vol 1,N01, online at http://idpl.oxfordjournals.org/content/1/1/28.full.pdf+html/ accessed 05.04.11

[22] Opinion of the European Data Protection Supervisor on the Communication from the Commission (2011) online at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf/ accessed 31.03.2011

[23] Id. no 20

[24] Data Protection and Privacy Commissioners *"Joint Proposal for setting International Standards on Privacy and Personal Data Protection"* (2011) http://www.privacyconference2009.org/dpas_space/Resolucion/common/resolution_international_standards_en.pdf / accessed 31.03.2011

[25] Lilian Mitrou "Privacy in Web 2.0" (2010), DiMMEE, 3/2010, page 319

[26] Premier Ministre de la République Française, 2010, Charte « Droit a l'oubli dans les sites collaboratifs et les moteurs de recherche», http://www.aidh.org/Actualite/Act_2010/Images/Charte_oubli_La_Charte.pdf and http://www.village-justice.com/articles/Internet-droit-oubli-numerique,9772.html / accessed 31.03.2011

[27] European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council the Economic and Social Committee of the Regions http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf , accessed 29.03.2011

[28] Giovanni Sartor and Mario Viola de Azevdo Cunh, 2010, "The Italian Google-Case: Privacy , Freedom of Speech and Responsibility for Users-Generated Contents", International Journal of Law and Information Technology Vol. 18, No 4, Oxford University Press online at http://ijlit.oxfordjournals.org/content/18/4/356.full.pdf/ accessed 05.04.2011 and Paul Mendez 2011,"Google Case in Italy" International Data Privacy Law online at http://idpl.oxfordjournals.org/content/early/2011/02/25/idpl.ipr003.full / accessed 05.04.2011

[29] Id. no 20

[30] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability on line at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf/ accessed 24.03.2011

[31] Information Commissioner's Office, 2009, "ICO PIA Handbook" on line at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html assessed 06.04.2011

[32] Lilian Mitrou "Privacy in Web 2.0" (2010), DiMMEE, 3/2010, page 319

[33] Dr. Cavoukian Information and Privacy Commissioner of Ontario, Canada, 2011, "Privacy by design resolution" on line at http://www.ipc.on.ca/images/Resources/privacybydesign.pdf accessed 06.04.11 and Data Protection and Privacy Commissioners – Resolution on Privacy by Design, Jerusalem, Israel, (27-29 October 2010), online at http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf /accessed 24.03.2011

[34] European Commission, 2010, "Agenda for Europe" on line at http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf / accessed 06.04.11

[35] Communication from the Commission to the European Parliament and the Council on *"Promoting Data Protection by Privacy Enhancing Technologies (PETs)"*, (2007), on line http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF accessed 10.04.11

[36] Final Report of London Economics to the European Commission DG Justice, Freedom and Security, about the study on the economic benefits of privacy-enhancing technologies, online at http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf / accessed 06.04.2011