Position paper

ETNO Reflection Document on the EC Public Consultation on the Framework Data Protection Directive

December 2009

Executive Summary

- ETNO[1] welcomes the EC public consultation on the legal framework for data protection and wishes to contribute to the important debate on the future of data protection in the European Union
- Data Protection is a Fundamental Right. The current EU legal framework introduced a high level of protection. However, in the light of the speed of technological change, some adjustments may be necessary to maintain the same level of protection of individuals' fundamental rights while, at the same time, improving legal certainty and flexibility for EU companies
- The basic principles of the Framework Data Protection Directive (Directive 95/46/EC) are still valid. The Madrid Resolution maintains the reference to the basic principles such as lawfulness and fairness, purpose specification, proportionality and data quality.
- Therefore, more than modifying the current Framework Data Protection Directive, emphasis should be put on ensuring harmonisation amongst Member States' national laws and effective implementation. Indeed, one of the main shortcomings of the Directive is that its implementation has not achieved the desired level of harmonisation amongst Member States. This lack of level playing field has affected European companies operating in various Member States, putting them in a competitive disadvantage.
- A "level playing field" should be granted for all entities that run websites and services which target European citizens, regardless to the fact that the controller has an establishment within the EU

1 ETNO aisbl, Avenue Louise 54, B-1150 Brussels – Register ID number **08957111909-85**

Introduction

The availability of super-fast broadband connections can play a vital role for Europe's economy and citizens by stimulating productivity growth across sectors, as well as preserving and creating employment in Europe. Very high-speed broadband will help to ensure Europe's long-term competitiveness and allow future participation of its citizens in the global information society.

These new networks are needed as the backbone for sustained growth of the industry to respond to the exponential growth of online traffic and to open up new opportunities for EU citizens and businesses, for example, creating and sharing digital content thanks to higher upload speeds, engaging in new forms of collaborative working online, taking advantage of future services such as distant health care, etc.

However it is not only in this context that the issue of "personal data protection" will become a crucial prerequisite for EU citizens to participate actively in a truly global information society, as pointed out by the European Commission. Indeed, with a view to the convergence of sectors, services and players, it is absolutely necessary to have a level playing field. In many cases providers of Information Society services compete more and more with the "traditional" European e-communications services and network providers, but are not subjected to the strict sectoral rules embedded in the e-Privacy Directive. Therefore **ETNO sees a growing need for a more homogeneous application of data protection principles to the benefit of users and also not to put European companies at a market disadvantage vis-à-vis global players,** which are subject to far less stringent privacy rules.

Specific Comments

In the context of the aforementioned crucial prerequisite for active participation in a global information society, ETNO wants to underline a number of key factors.

Level playing field

The electronic communications sector is submitted to a heavy and burdening sector-specific regulation (Directive 2002/58/EC, e-Privacy Directive, whose review process has just been finalised) in addition to general regulation (Framework Data Protection Directive). This however is not the case for other economic sectors such as the financial sector or the energy sector, which are also vulnerable and very critical.

Furthermore, with a view to the convergence of sectors, services and players, it is absolutely necessary to have a level playing field. If we think about **providers of Information Society services** competing more and more with the "traditional" European e-communications services and networks providers, they are not subjected to the strict sectoral rules embedded in the e-Privacy Directive (and its just finalised review). As an example, the obligation to notify security breaches (Art. 4 of the new ePrivacy Directive) only applies to e-communications service providers, when in most cases providers of Information Society services do collect and process huge amounts of personal data.

Given the development of new technologies and Internet-based applications like behavioural advertising, localization or social networking, there is a growing need for a more homogeneous application of data protection principles to the benefit of users. This will avoid putting European Companies at a market disadvantage vis-à-vis global payers, which are subject to far less stringent privacy rules.

The assumption, with these applications, is that data processing has no geographical borders and that EU citizens should be granted the same degree of protection irrespective of the origin / location of the service provider.

Indeed, a critical issue relates to the definition of the applicable law in the case in which data of European citizens are processed by extra-UE entities thanks to electronic and non-electronic facilities/equipment that are placed outside the EU borders.

As a matter of fact, this creates profitability for companies that are based abroad with a negative effect on the European productivity and economic growth. A "level playing field" should be granted for all subjects which run websites and services which target European citizens, regardless to the fact that the controller has an establishment within the EU.

With regard to the applicable law when the data controller is not established on EU territory, the current criteria of use of equipment situated within the EU should be substituted and the criteria of "services targeting EU citizens" should prevail.

International Transfer of Data

Current rules for international transfer of personal data[2] outside of EEA are cumbersome, therefore they should be updated and simplified taking into account the new economic reality European Companies are facing.

Binding Corporate Rules solutions for inter group transfers are equally cumbersome and should be made simpler for groups of companies to adopt. Notwithstanding the potential of BCR, experience has shown that being too cumbersome, they are not fit for purpose.

It is therefore necessary to find solutions to solve the problems met by groups of companies in case of international data transfers. A possibility could be to use the concept of mutual recognition or to develop the concept of "**Group of Companies**".

The Directive did not consider the concept of "Group of Companies" and any transfer of data between different entities of the same group is considered as a data transfer towards third parties. Needles to say, that this situation creates a significant and unnecessary burden for the companies.

For the first time, the Madrid Resolution refers to "transfer carried out within corporations or multinational groups". ETNO welcomes the recognition of such economic reality and asks the EC to consider this new approach in connection with data protection rules.

ETNO believes that different entities of a certain corporate structure shall be considered as one single entity for the transfer of personal data between them.

In order to facilitate the transfer of data within a given corporation, the internal privacy rules of the Corporation should provide the guarantees that the transferred personal data will benefit from the same level of protection than the one existing in the European Union or EEA.

Such an approach would imply that instead of considering the data transfers adequate or not based on the country of destination, the assessment of adequacy would be based on the accountability of the

2 Art. 25 of the Data Protection Framework Directive

data controller. Irrespective of whether the data transfer is within the same EU Member State, within the EU/EEA or outside the EEA, the data controller would be held liable for the protection of personal data.

This approach is especially relevant in a **cloud computing** scenario. The geographical reference disappears. No matter where the data are stored, the data controller remains responsible. It is up to the data controller to set the contractual provisions with the necessary guarantees and to verify that these rules are respected by the data processor. Technological developments such as cloud computing should not be constrained by legislation.

In order to facilitate data transfers, another important point is to **limit the obligation to notify the supervisory authority**. Again, making reference to the Madrid Resolution, the Resolution does not even mention the need to notify. Notification is not, and should not be, one of the basic requirements, although some national laws transposing the Directive 95/46/EC have introduced an extensive interpretation of the use of notification procedures. Besides the national rules imposing an extensive use of notifications, some National Data Protection Agencies have abused of such requirement. Consequently, the lack of harmonization when transposing the Directive has resulted in a lack of a level playing field within the EEA. As an example, in Spain notification to the NDPA was made compulsory in any case of transfer of data, not only to third countries, but even within the EU or within the territory of Spain itself. This very restrictive interpretation of the Directive amounts to an effective barrier to the "free flow of personal data between Member States", which was one of the aims of the Directive back in 1995 (Art. 1.2.).

Need to limit the notification obligations

Above we have referred to the notification in case of data transfers. Another important issue is the obligation upon data controllers to notify the supervisory authority of any processing operation (Art. 18 Directive 95/46/EC). Experience shows that mandatory notifications to NDPAs have not contribute to more transparency towards data subjects, while they do imply an important administrative burden for data controllers. Limiting, or simply deleting, the obligation to notify would imply that data controllers can focus on "effective" data protection compliance instead of devoting important resources to comply with "formal" notification obligations. The same would apply to the limited resources of National Data Protection Authorities, which have to dedicate teams to follow the notifications. Eliminating

unnecessary formal requirements will liberate time and resources of both data controllers and NDPAs.

Accountability, compliance and transparency (elements which would justify the need for notification) can be achieved in other ways, such as by a clear privacy policy, in which the data controller communicates its principles and commitments. For the data subject, having a clear and easy to reach and read privacy policy will be much more effective than having to consult the supervisory authority's data bases.

Data controller and data processor

The distinction between data controller and data processor is more and more blurred, especially in the complex online environment, for instance, in case of companies outsourcing the processing of data or in a cloud computing scenario.

Therefore, the responsibilities of both parties should be reconsidered as in more and more cases there are several parties that can be defined as "data controller" as they determine "the purposes and means of the processing" (Art. 2 of the Directive). Rules of liability of the data controller should be made more flexible and contractual clauses between the data controller and the data *processor* could set the liabilities of each party as in many situations, the data *processor* will be the only responsible for the data quality and data security and not the data controller anymore. Both parties are increasingly considered as 'joint controllers' with different responsibilities.

Codes of Conduct

In an area such as Data Protection, which is heavily regulated and where an important set of legislative measures does already exist, it is not easy to assess the added value of Codes of Conduct.

Furthermore, due to the lack of harmonisation at the EU level, Codes of Conduct have not been used often. Indeed, in order to have any added value, a Code of Conduct should introduce something more than what is already established by law. Considering the existence of great differences between national data protection laws transposing the Framework Directive, individual companies have not been inclined to develop sectoral Codes of Conduct.

EU Trustmark

ETNO supports a non-binding system of European trust marks/labelling aimed at incentivizing companies that invest in an enhanced reliability of data processing. It is our conviction, in fact, that compliancy with privacy rules will be, on the one hand, a relevant opportunity for business and, on the other, will enhance consumer trust and confidence. In a perspective of ameliorating customer trust and therefore pursuing the best possible relation with customers, ETNO sees a labelling system as an important quality objective for the European e-Communication Industry and a possible global market advantage given the high level of European data protection standards.

Education and Awareness raising initiatives

For data protection rules to be effective, it is of utmost importance that the data subjects are aware of the privacy impact of their behaviour in the online environment. More and more data subjects realise the importance of protecting their privacy by themselves (e.g.: by not sharing certain information in a social networking site). As an example, in February 2009 Facebook was forced to withdraw changes of its previous terms of service regarding user data as a consequence of the protests of its users. Facebook users became aware of their rights and reacted accordingly.

Education and Awareness raising campaigns should be developed in collaboration between private actors and public administration.

Data Protection rules should apply also to Public Authorities

With the entry into force of the Treaty of the Functioning of the EU (TFEU) on 1 December 2009, the application of EU Data Protection will have a more horizontal and comprehensive approach: they shall apply not only to the private sector (e-communications service providers) but to the Public Authorities as well.

Until now, Law Enforcement Agencies have often benefited from exceptions when processing personal data, so that they are excluded from the application of Data Protection rules. As an example of this different treatment, the **Council of Europe draft recommendation on online profiling** (discussed at the 25th CoE Plenary meeting beginning of September) establishes a broad exception for the public sector. With the Lisbon Treaty this difference should disappear.

Concluding Remarks

Data Protection is key for ETNO companies' brand reputation. Business depends on Consumer Confidence and new business models such as behavioral advertising rely more and more on the use of personal data.

At the same time, data protection issues are not black and white and require careful case by case assessment. Today all stakeholders face an important challenge as the right balance needs to be found between the protection of EU citizens' personal data and the legal certainty and flexibility for businesses. Future data protection rules at the EU level should go hand and hand with other EU objectives such as the achievement of the EU single market and the consolidation of EU business competitiveness worldwide. It is absolutely necessary to avoid that EU companies are in a competitive disadvantage vis-à-vis companies from third countries.

The global and open dimension of the Internet demands global standards for data protection. Considering that the Internet does not have any barriers, legal systems should not create them. In light of new technologies and globalization, cross-border flows of personal data will increase more and more, therefore it is of utmost importance that data protection rules are not developed in an isolated manner.