ID REGISTER: Telef05162

TELEFÓNICA'S REPLY TO THE EC PUBLIC CONSULTATION ON THE COMMUNICATION ON A COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

Introduction

Telefónica welcomes the opportunity provided by the European Commission to be able to convey our point of view on the reform of *Directive 95/46/CE of the European Parliament and the Council dated 24th October 1995, on the protection of individuals regarding the processing of personal data and the free movement of this data*[1] (hereafter referred to as the DP Directive), via this Public Consultation, whose ultimate goal is to modernize the legal system of the European Union in the area of protection of personal data, taking into account that, as pointed out by the "Communication on a comprehensive approach on personal data protection in the European Union" (hereafter referred to as the Communication), *"the speed of technological change and globalization have profoundly altered our means and have introduced new challenges in the area of the protection of personal data".*

The protection of personal data is a fundamental right of individuals, contained in Article 8 of the Charter of Fundamental Rights of the European Union. Telefónica considers that the twofold objective of the Directive (the protection of the rights and fundamental freedoms of persons and free movement of personal data in the internal market) remains perfectly valid, as the Communication itself also restates in its first paragraph. At the same time, Telefónica agrees with the European Commission that there are certain issues in the current law that require a thorough review, by all stakeholders involved, to reflect on an update of the concepts in order to establish a renewed legal framework that meets the needs and demands raised by the new digital environment and which serves as a reference in the international arena.

[1] Directive 1995/46/EC, dated 24th October, by the Parliament and Council, on the Protection of individuals with regard to the processing of personal data and the free movement of such data.

However, the technological neutral nature of the Directive should be maintained and, even more, reinforced. Over the past 15 years, the current technology-neutral approach of the Directive has provided a broad framework to be applied to different emerging technologies that were not even foreseeable back in 1995. Any future review of the legal framework should enable innovation and avoid discrimination between different technologies. These premises would only be possible if the technology neutral feature of the Directive is maintained and the Directive remains flexible. As a matter of fact, technology will continue to change, therefore the legal framework should not refer to any specific form of technology, otherwise we run the risk that the rules will become obsolete very quickly.

A key objective should be to ensure that individuals can benefit from a harmonized, transparent and consistent treatment of their personal data, irrespective of the geographical location or the economic sector of the data controller, or what business model or technology is used.

For this purpose, Telefónica is offering the European Commission some proposals on how we think new challenges taking place on the technological, economic and social level must be handled, based on the respect for the rights of individuals and the promotion of the internal market.

Key issues:

- Telefónica believes that Directive 95/46 has been an effective piece of legislation, aimed at achieving the difficult **balance of protection individuals' rights while ensuring the free flow of data in the internal market. Both objectives remain valid** and should be put on an equal foot.

- One of the main shortcomings of the Directive has been the divergent national implementations and divergent interpretations, which have result in a lack of harmonisation negatively affecting individuals and businesses. Therefore, any review process should put **emphasis on ensuring more harmonisation both in its transposition and its implementation amongst Member States, avoiding an overly prescriptive approach**.

- The **technological neutral nature of the Directive needs to be maintained** in order to achieve a future proof legal framework.

- Telefónica calls for a **necessary reduction of administrative burdens on data controllers**, which do not provide any real benefit neither for the NDPAs nor for the data subjects. With the aim of reducing red tape, clear company's internal privacy policies, easily accessible and based on Transparency, Information and Choice can be more effective for end users and require fewer resources.

- Focus should be put on **reducing complexity and costs associated with the current rules for international data transfers** inside and outside the European Union. The **concept of "group of companies" should be recognized** as companies are increasingly organized on a global scale and apply common security and privacy policies which guarantee seamless high standards of protection of customer's personal data.

- Last but not least, the review should aim at **achieving a truly level playing field for all data controllers both in off-line and on-line environments**. Irrespective of the geographical location or the economic sector of the service provider, EU citizens' personal data shall be granted the same level of protection. Otherwise, inconsistent application of the EU rules has a clear negative impact on competitiveness of EU companies and on individuals trust and confidence.

- Finally, the EC should take into account that overly prescriptive and inflexible consent requirements should not impede innovation and development of new services and consumer choice.

For ease of reference, herewith we provide more detailed input following the headings used in the Communication.

Comments on the EC Communication

1. Strengthen the rights of individuals

a. Ensure adequate protection of individuals in all circumstances

The technological development and innovation that society is currently experiencing, immersed in a globalized world and in a digitized environment, has created new patterns of behaviour in individuals and has, in some cases, opened new questions. However, notwithstanding this, we believe there is a general consensus that the general core privacy and data protection principles already established remain alive and more than ever should be applied to all economic and social activities and to all actors processing personal data, also in digital environments.

In the Communication, the Commission notes the benefits of the approach taken to the definition of Personal Data, not least, flexibility to deal with developments. We believe that whilst this flexibility can sometimes be beneficial, it can also create uncertainty. Hence it is also

important that the framework should enable organisations to take a practical, proportionate and contextual approach to protecting individual's interests.

b. Increase transparency for stakeholders

Telefónica supports the introduction, in the EU legal framework, of a principle that encourages transparency since we believe that this is an initiative that will allow the data subjects to better control and manage their own data, thus making them participate in decisions affecting their privacy.

Nevertheless, we must be aware of the fact that society in general and the information society, in particular, encompass an infinite number of very diverse products and services that need to adapt the characteristics of each service to the requirements of transparency and information. Therefore, whilst Telefónica is in favour of good practice guidance regarding the development of privacy information notices that take into account the specific needs of users depending on the type/ context of product or service they use, we also would caution against prescriptively specifying one form of privacy information notice to apply to all data collection and products and services regardless of context. We believe a "one size fits all" approach is inappropriate here and will not enable organisations to delivery transparency in a meaningful and contextual basis to individuals (thus enabling better management of their data).

Within this initiative, special attention should be paid to the topic of minors who require special protection in the processing of their personal data which must be dealt with in a uniform manner in all European legislation.

The protection of minors and, in particular, their participation in the online world, is one of the pillars of Telefónica's Corporate Social Responsibility policy. Telefónica has developed electronic communications services specially designed for children such as Kangaroo Net, Kangaroo mobile, Playpack, etc. as well as parental control mechanisms that allow parents to sign up for network monitoring products[2].

The Commission should encourage players who operate Information Society services to develop mechanisms for protecting childhood in the on-line world, which are effective in verifying whether a child's maturity allows him/her access without the aid of their parents or tutors. These mechanisms should be effective but also flexible and proportionate to any privacy risks for the child, so as not to constitute a disproportionate

[2] We will be pleased to provide more detail about these initiatives if that would be helpful.

hindrance to the creation of new services. For example, in those situations in which children are legally allowed to accept responsibilities and meet obligations, they should be also allowed to accept or refuse the use or their personal data, so that we can reach an adequate level of consistency between their rights.

c. Strengthening control over one's own data

Telefónica considers it important to grant data subjects control over their own data as the current framework provides. In addition, it is important that there is clarity and understanding as to how those existing rights apply in an evolving digital world and so we believe the Commission is right to consider this area further (and if it is necessary to provide individuals with different options that are adapted to their particular interests and in a uniform way in all Member States). It will be important to determine whether strengthening of rights is really necessary or rather whether it is more appropriate to clarify how those rights apply in the areas that have give rise to query/ concern. –For example, exercising the rights to access, correction, erasing and blocking, already provide significant control mechanisms for data subjects and so it may be that clarification is simply needed as to their application in certain circumstances. We would caution against "re-inventing the wheel". However, to achieve full efficiency it may be necessary to analyze the situation in each Member State regarding these rights and seeks a uniform formula for the entire European Union.

Regarding the principle of data minimization, we believe that it is already contained and therefore sufficiently established in Article 12 of Directive 95/46/EC. Therefore, it may not be necessary to strengthen it from a policy perspective but from the point of view of its effective practical enforcement.

We also believe that data minimization is a core element by "privacy by design" and should be better addressed as a part of the design.

Regarding the right to be forgotten, Telefónica does not believe that it produces any new features with regard to the rights of opposition or cancellation. Thus we consider it more of a priority and more efficient to focus on harmonizing the rights of access, correction, cancellation and opposition and ensuring that all online service providers processing personal data do effectively apply this principle.

The right to be forgotten is not a new concept and we can find it in the current DPD combining some of the articles setting the basic principles for the legitimate processing of personal data. Indeed, basic principles on Data Quality (art. 6), Right of access and Right of rectification (art. 12)

and Consent (art. 7) ensure which is now named as the new "right to be forgotten". Telefónica considers that the current framework is always valid and that there is no need to "re-invent" the existing safeguards.

Article 6 establishes the principle relating to Data Quality, based on which the processed personal data must be adequate, relevant and not excessive for the purpose for which they are collected and processed. The personal data must also be accurate and kept up to data when necessary.

Furthermore, Article 12 guarantees that every data subject has the right to obtain from the data controller information about their personal data being processed as well as ask the data controller for rectification, erasure and blocking of their personal data when their processing does not comply with the provisions of the law, in particular, in case of data being incomplete or inaccurate.

Finally, Article 6 establishes the legitimacy of the processing of personal data when the data subject has given his consent, amongst other reasons for justifying the processing.

These principles have been implemented in national legislations in Member States (eg.: in Spain) in a way that data controllers must always respond to these requests to access the processed data or to rectify them, unless there is an justified reason for not doing so[3]. Furthermore, these rights are reinforced by redress mechanisms that give individuals the right to request a data protection authority to assess any refusal to erase personal data as well as the possibility to pursue any such refusal via the Courts.

Finally, it should be pointed out that the so-called right to data portability encompasses two types of rights. On one hand, we have the right of cancellation, already enshrined in Article 12 of Directive 95/46/EC, and as previously mentioned, requiring a harmonized revision across the EU and on the other hand, the right to portability, strictly speaking, whereby data subjects can order the data controller, to transfer their data to another data controller. With regard to the latter right, Telefónica recommends that a comprehensive study be carried out on the consequences that the latter might generate since, in our opinion, the disadvantages may outweigh the benefits. We might find situations in which the possible technological inequality and security of the information existing between the data controllers may cause prejudice to data subjects or even third parties. A clear example of this situation can be found in social networks, in which data subjects may post photos in which third parties can appear who probably have consented to appearing in their images on this specific

[3] Again, mentioning how the Directive has been transposed into national Law in Spain, we would like to stress that the right of access is free of charge for the data subject.

social network and not on another so they could oppose the right of portability exercised by the primary data subject. Instead of enhancing control over one's own data, Data Portability could imply less control to individuals over their personal data.

d. Awareness

As previously mentioned, the protection of personal data is the responsibility of data controllers and data processors as well as the data subjects. In other words, it involves a shared responsibility which requires that precautions and security measures be taken by both sides.

In this respect, the education policies at the European Union level and at the national level, as well as the actions promoted by the Data Protection Authorities in each Member State and by the Art. 29 Working Group on awareness, training and education that educate citizens how to have control over their own personal data and protect their privacy would be crucial.

e. Ensure free and informed consent

We all recognise that consent has become more complex over time and that the clarity of consent may need improvement. Furthermore, the reality of an online interaction, delivered in today's technology, does not provide the opportunity to meet all of the legalistic consent requirements. Therefore, Telefónica welcomes the initiative by the Commission regarding the clarification (and harmonization) of the rules governing users' consent to the processing of their personal data, provided it is not raised as an isolated measure to hinder the providing of consent by users, transforming a free and informed consent into an express or written consent. This situation would slow down and impede the free movement of personal data in information society, which is characterized by its dynamism and its constant development, harming all parties that interact in it.

Therefore, rules on consent must be governed by the principle of flexibility in the way it is provided and accompanied by a series of additional measures that will enable their effectiveness, such as the principle of transparency, awareness or information, as noted above.

As the European Data Protection Supervisor, Peter Hustinx, recently said[4], consent should not be overestimated. This statement is in line with the Directive itself, which in its Article 7 also sets the possibility of processing of personal data in other cases, even without the consent of

[4] Peter Hustinx used this expression at the European Parliament Privacy Platform debate, which took place on 1st December 2010.

the data subjects (eg.. processing is necessary for the performance of a contract, for the compliance with a legal obligation, etc.).

Therefore, rather than focussing on consent at the expense of other opportunities to enhance a user's privacy experience, we believe that a key objective should be to develop and reinforce the mechanisms by which users can make informed choices depending on the context of specific uses of data. For example, a person requesting a location based information service to locate the nearest automatic teller machine, is actively asking to be located, and should not be required to negotiate cumbersome, lengthy legalistic privacy notices by which they may indicate their 'unambiguous explicit consent'. Such impositions would damage the user experience and do little, if anything, to enhance the user privacy experience.

Different browsing settings allow for selections of preferences and graduated choices which allow some flexibility in what and how personal data is collected, used, retained or shared.

f. Strengthen the effectiveness of remedies and sanctions

In our view, the system of sanctions stipulated in Directive 95/46/EC requires an urgent review to ensure a uniform and homogenous system within the European Union.

Experience shows a wide disparity between the various systems of sanctions. This disparity is even reinforced by differences in sector specific regulations, such in the case for the electronic communications sector, which adds extremely demanding obligations to this sector's actors. Even other sectors, such as the health care or the financial sector, which handle very sensitive data, have a system of sanctions that is much less strict.

Therefore, e-communications service providers do not enjoy equal treatment within the European Union since they have to face very different systems of sanctions depending on the Member State where they are based and regarding the sector specific legislation. This in turn results in a huge discrimination based on issues of nationality and sector, which adversely affect the scope of the internal market.

In any case, the strictest system of sanctions would be useless if it were not accompanied by actions designed to raise awareness.

2. Enhancing the internal market dimension

a. Increase legal certainty and guarantee a level playing field for data controllers

The free movement of personal data in the internal market, one of the two objectives of the Directive 95/46/EC, is not possible unless you achieve a certain degree of harmonization of data protection national laws in Member States. The differences, in some cases minimal but in others substantial, generate legal uncertainty due to issues of territoriality and unjustifiable economic inequalities for companies established in various Member States.

In our opinion, the differences between national legislation within the European Union caused by the degree of autonomy granted by Directive 95/46/EC to the Member Status should be corrected, at least with regard to the rights and obligations of the parties concerned, so that any person, whether it be a natural personal or a legal person, residing in a Member State, does not see their legal rights diminished due to lack of harmonisation and divergences in the transposition and interpretation of the Directive at the national level.

Finally, we would like to point out that data protection laws should be enforced in a coherent and harmonised way involving all services of the Information Society, in other words, for all new players that take part in ICT and not only for telecommunications operators. Traditional telecommunications companies are nothing more than "one more player" in the global landscape of ICTs, in which other information society service providers (content providers, search engines, etc.) do exist and compete with e-communications service providers, whose level of compliance with the requirements of the rules on personal data protection is considerably higher. Strong differences in the way privacy and data protection principles are implemented and enforced amount for breaking the necessary level playing field between operators and discrimination between European citizens.

Therefore, first and foremost, we consider it necessary that all companies who, in the new on-line environment, offer their services whether off-line or on the web to European citizens comply with the EU rules on personal data protection, irrespective of where they may be providing these services or where they are located (for example, outside the EU). Current experience shows that EU data protection rules are effectively applied only to European based companies. Otherwise companies in the EU are at a competitive disadvantage in relation to other players in the world, which are subject to less stringent data protection laws or weaker applications regime. This equal treatment of personal data is essential from the

perspective of the end-user: EU citizens must be able to enjoy the same level of protection for their personal data, irrespective of where the service provider is located.

For example, current EU framework is no neutral in respect business models placing discriminatory obligations and restrictions on electronic communication service providers when they are dealing with some personal data as "traffic data" and "location data" and by the contrary, releasing these burdens to other on line businesses which collect and use equivalent information about consumer data traffic on line and about their geographical location.

b. Reduce the administrative burden

Telefónica supports the reduction of administrative burdens that we understand should instead be replaced by promoting initiatives involving self-regulation. (See section 2.e)).

Data Protection should not impose excessive regulatory burdens on industry which, in turn, may be counterproductive to the aim of enhancing customers' trust and confidence. This is the case of the current rules imposing on data controllers the obligation to notify the National Data Protection Agencies of any processing of personal data. Such an obligation requires important financial and organisational resources from companies as well from supervisory authorities (which must monitor important amounts of notifications) without providing any real benefits for the data subjects.

Telefónica believes that each data controller needs to define a clear privacy policy, easily accessible for all customers and stating the principles of the data processing. Such an approach would be more effective for end users and would require fewer resources from data controllers and data protection authorities

c. Clarifying the rules regarding the applicable law and Member States' responsibility

Telefónica supports the Commission's initiative to improve the wording of Article 4 of Directive 95/46/EC, concerning the determination of the applicable Law since the current wording raises doubts, especially in those situations in which a company, such as ours, established in several Member States, is forced to duplicate efforts and resources since it does not know for certain which is the applicable Law.

In this respect, Telefónica welcomes the recently adopted Art. 29 WG Opinion 8/2010 on Applicable Law when referring to the need for

additional criteria, in cases when the controller is established outside the EU but it is "targeting EU individuals". Such a new criterion will help to achieve a truly level playing field for all online service providers running websites and providing services which target EU citizens. This will also increase citizens' confidence that their personal data are handled correctly in any circumstance.

Moreover, the geographic dimension is increasingly diluted within the Information Society. The increasing geographic dispersion that on-line services generate creates a situation whereby we are faced with extremely complex situations. It is no longer a problem for the European Union or for Member States alone, but rather a problem of an international nature.

Therefore, Telefónica encourages the European Union to target its efforts also towards the development of some international rules or standards aimed at more uniform implementation of data protection universal principles.

d. Strengthen data controllers' responsibility

Telefónica is in favour of strengthening the responsibility of data controllers as well as data subjects' responsibility, provided this does not increase the administrative burden and result in a slowdown in the delivery of products and services to users of the information society. This would imply a clear anti-competitive disadvantage for EU companies with respect to the global market.

As stated in Opinion 3/2010 of the Article 29 Working Group[5], Telefónica considers necessary the inclusion of a principle of accountability in the review of the Directive. This principle would encourage data controllers to adopt effective measures providing genuine data protection that would complement and strengthen some of the legal measures envisaged by the Commission. Off all the measures being considered, Telefónica opts for selecting those strategies and procedures that streamline business and provide a comprehensive response to an interconnected world, such as promoting the use of technologies designed to protect the right to privacy (PET) and for adding the principle of "privacy by design", prior to launching any product or service, as key elements for identifying and neutralizing any potential threats to individual privacy.

However, Telefónica would like to stress the need to apply both tools in a flexible and tailored manner. Both mechanisms need to be adapted to a given organization's needs. Privacy by design and use of PIAs, as a

[5] Article 29 WG's Opinion 3/2010 on the principle of Accountability, adopted on 13th July 2010.

mechanism of assistance and self-regulation for the companies themselves, should be generalised without trying to dictate or over regulate how the design objectives are to be met or the specific content or application of the PIA.

Despite the fact that the existence of a Data Protection Officer could be appropriate in some organization and even mandatory in certain countries, we consider that companies should have flexibility to choose between other ways to organize their internal Data Protection principles and programs. To make mandatory the appointment of a Data Protection Officer could be an excessive burden and disproportionate, especially for small and medium-size companies, whose task, we feel, is already covered in Article 18 of Directive 95/46/EC.

e. Promote initiatives in the area of self-regulation and explore the possibility of EU certification schemes

As we have indicated in section 2. b), Telefónica is very much in favour of promoting self-regulation whether it be at the global, sector or corporate level.

To this end, the revision of the Directive 95/46/EC should consider more incentives for assuming codes of conduct and privacy policies within companies.

In this sense, we can mention how important will be to support self regulatory approaches which create a culture of respect information privacy and at the same time establishing a framework that provides transparency and opportunities of choice to promote new services as "personalised advertising" services or "location- based –services".

The implementation of all of these ideas, coupled with increased awareness amongst consumers could further empower users to make their online decisions based on the security of their data.

3. Review the data protection rules in the area of police and judicial cooperation involving criminal matters

The experienced gathered by industry shows a clear trend that data retention obligations for Law Enforcement purposes, go far beyond the real needs and requirements of the Law Enforcement Authorities.

Likewise, it would be recommendable to conduct a thorough review of the types of data to be retained and the periods of retention imposed on e-communications services providers by the Directive 2006/24/EC on Data Retention[6].

4. The global dimension of data protection

a. Clarify and simplify the rules for international data transfers

From the point of view of a Group of companies established in various Member States and outside the European Union as Telefónica, we feel it is very necessary from a regulatory standpoint to eliminate obstacles in the international transfer of data between companies within the same Group, provided the Groups of companies guarantee the existence of privacy policies that rigorously enforce the principles contained in Directive 95/46/EC.

The EU legal framework should recognise the concept of "group of companies" in order to facilitate the transfer of data between members of the same group. This would be an important step in reducing the administrative burden of EU businesses.

For the first time, the Madrid Resolution of November 2009 made a reference to "transfer carried out within corporations or multinational groups". Internal Privacy Policies of such multinational groups would then include the guarantees that the transferred personal data will benefit from the same level of protection as if they were processed within the EU borders.

In order to facilitate international data transfers, another important measure would be to limit the obligation to notify the Data Protection

[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of public electronic communications services or of public communications networks amending Directive 2002/58/EC (Official Journal L105 of 13.4.2006)

Agency. The Madrid 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. Furthermore, besides the national rules imposing an extensive use of notifications, some National Data Protection Agencies have abused such a 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 compulsory in any case involving transfer of data, not only to third countries, but even within the EU or within the territory of Spain itself as well. This very restrictive interpretation of the Directive amounts to an effective barrier to the "free flow of personal data between Member States" (Article 1.2. of the Directive).

b. Promote universal principles

As already mentioned, there is a demand for harmonization between the various European regulations but also for a regulatory approach between the regulations of countries such as the United States, India, Japan..., considering that the harmonization of general principles will constitute a driving force behind World Wide Commerce as well as an economic incentive worldwide. See point 2.c.

The European Commission should become the driving force behind the development and promotion of international standards, considering the high level of protection of personal data in the European Union.

The creation of the most harmonised framework possible for data protection at the global level would contribute to the development of world trade. It would facilitate the exchange of information between the various economic players as well as the processing of data by companies that are operating in the various countries, with the ultimate result of a higher level of protection of the Fundamental Right to privacy.

Likewise, achieving a more aligned framework between the different countries could help the various companies to increasingly consider the level of protection requested by end users within their own competitive strategies, so that a clear incentive exists for compliance with these levels.

5. Strengthen the institutional arrangement for better enforcement of data protection rules

Telefónica considers it necessary to ensure better enforcement of data protection rules that would imply two actions:

- harmonize and clarify the rules governing the role, powers and competences of national data protection authorities and

- encourage greater cooperation and coordination between the national data protection authorities and ensure that there is a clear channel for dialogue and engagement with industry.

January 2011