

The Lisbon Treaty and the Protection of Personal Data in the European Union*

by *Alfonso Scirocco*

The Lisbon Treaty, signed on 13 December 2007, brings fresh air not only to the future of the European Union in general, but also to the relevance of fundamental rights - and in particular the right to the protection of personal data – within this renewed legal framework.

The new Treaty puts an end to the period of reflection that started in 2005 further to the negative results in France and the Netherlands of the referenda on the Constitutional Treaty. Even though a consolidated version will be available only once the Treaty enters into force – on 1 January 2009, assuming that no problems arise in national ratifications – a careful analysis of the current “user-unfriendly” text reveals that most of the elements of the controversial Constitution for Europe have been incorporated in this reform treaty. Indeed, the main developments envisaged by the Constitutional Treaty can be found in the Lisbon Treaty, apart from some minor or even cosmetic changes, such as the ban on the word “constitution”, the lack of references to the European symbols (anthem, flag) and the non inclusion of the Charter of Fundamental Rights in the Treaty itself.

This is certainly the case with regard to the provisions relating to the protection of personal data, which should be read in the broader context of the enhanced recognition of fundamental rights and of the major improvements in the provisions on the Area of Freedom, Security and Justice.

In order to better understand the enhancements brought by the Lisbon Treaty, it is necessary to briefly recall the current legal framework governing the protection of personal data in the European Union.

The current data protection legal framework in the European Union

According to the basic principle that European Union institutions may act only when the Treaties grant them the power to do so, the main pieces of legislation relating to the protection of personal data have been adopted, starting from 1995, on the basis of Article 95 of the European Community Treaty. This Article grants European Union institutions the power to harmonize the internal market, through the co-decision procedure, which entails a joint decision of the European Parliament and the Council.

Both the Data Protection Directive (95/46) and the Directive on the protection of privacy in the telecommunications sector (97/66, replaced by 2002/58) are therefore born on the grounds of a generic and horizontal legal basis, as necessary instruments of the completion of an internal market in which goods, services, capitals and workers should circulate freely. This means that these instruments are based on legal grounds primarily designed to address internal market harmonization – rather than fundamental rights – and that they are not meant to apply to the processing of personal data relating to the field of state security and judicial and police cooperation, even though many member States have decided to implement their main principles also to the latter activities.

The case law of the Court of Justice has later clarified their scope of application, on the one hand favouring an interpretation that takes into account the right to data protection even beyond the concrete exercise of economic activities (cases *Rechnungshof* and *Lindqvist*), on the other hand confirming the unsuitability of these instruments to cover those cases where personal data are processed for law enforcement purposes (*PNR case*).

Similar restrictions apply to the current Article 286 of the European Community Treaty, which was added in 1997 by the Amsterdam Treaty so as to extend the application of data protection principles also to personal data processed by European Community institutions and bodies. In this perspective, detailed provisions based on this Article were laid down by Regulation 45/2001, which also established a supervisory authority at Community level, the European Data Protection Supervisor.

As opposed to the high level of harmonization reached in the “classical” activities of the European Community (the so-called “first pillar”), the activities of the European Union in the fields of the

* Originally published in the digital magazine [Dataprotectionreview.eu](http://www.dataprotectionreview.eu), Issue 5, February 2008.

< <http://www.dataprotectionreview.eu/> >

Common Foreign and Security Policy (“second pillar”) and of the Police and Judicial Cooperation (“third pillar”) do not benefit from any general framework on the protection of personal data. Indeed, the European Union Treaty has not provided so far for any legal basis for data protection in the second pillar, while in the third pillar Article 30.1.b of the European Union Treaty merely refers to the necessity that initiatives involving exchanges of information between law enforcement authorities be subject to adequate provisions on the protection of personal data.

This background has entailed that no data protection rules are laid down for the Common Foreign and Security Policy, while the provisions relating to data protection in the third pillar are very fragmented and inhomogeneous, since they refer to the specific instrument they are included in (examples can be found in the recent proposals on exchanges of criminal records between Member States, or on the exchanges of DNA, fingerprint and vehicle registration data pursuant to the so-called “Prüm initiative”). This lack of harmonization increases even more if one considers that the Court of Justice currently enjoys limited powers in third pillar matters.

This situation strongly contrasts with the recent European Union activism in fostering processing and exchanging of personal data in order to combat crime and to fight terrorism. In this context, it is evident that the principles of Council of Europe Convention 108 – signed by all European Union Member States and laying down data protection rules applicable also to police and judicial cooperation – are not sufficient in this context and thus need to be further specified and integrated by the European Union legislator. Unfortunately, a proposal made by the Commission in 2005 to harmonize data protection in this area has not been adopted yet.

In conclusion, the current situation shows that the provisions of the European Community Treaty and the legal instruments adopted thereof seem solid enough to support the development of the internal market. On the contrary, the lack of harmonization of data protection rules in the other pillars of the European Union strongly affects the development of a European Union Area of Freedom, Security and Justice and may also question the legitimacy of some activities of the Common Foreign and Security Policy, such as the management of terrorists' blacklists (cases *OMPI* and *Sison*).

Furthermore, some recent phenomena like the use of commercial data for law enforcement purposes, as well as the increasing public/private partnership in combating crime, have blurred the borders between the different European Union pillars, at the same time triggering legal uncertainty and a time-consuming litigation before the Court of Justice (as in the cases of transfers of PNR passengers' data, or the retention of telecommunications data).

The changes in the Lisbon Treaty: new horizons for data protection in the European Union?

Against this background, the Lisbon Treaty brings a very welcome major improvement: the abolition of the pillar structure. The Treaty on the European Union, together with the Treaty on the functioning of the European Union, will provide a common legal framework for all the activities of the Union, abolishing the former divisions between more classical “Community” activities and more intergovernmental “European Union” fields of action.

The new general provision on data protection

This structural change is reflected also with regard to the protection of personal data. Article 16 of the Treaty on the Functioning of the European Union[†] lays down a specific and comprehensive legal basis, which is now prominently placed in Title II on “Provisions of general application”. The substantive parts of this provision clearly affirm that “Everyone has the right to the protection of personal data concerning him or her” (paragraph 1) and that compliance with data protection rules shall be subject to the control of independent authorities (paragraph 2). The European Parliament and the Council will jointly define the data protection rules relating to the processing of personal data both by Union institutions (and bodies) and by Member States when carrying out activities

[†] References are to the new numbering of the Treaty on the European Union and the Treaty on the Functioning of the European Union, which will substitute the numbering of the Lisbon Treaty, according to the tables of equivalences contained in its Annex I. See OJ C 306 of 17.12.2007.

which fall within the scope of Union law (paragraph 2).

There are many aspects to be welcomed in this new provisions: a subjective right to the protection of personal data is now explicitly included in the Treaties; the “constitutional” need for rules on data protection and for their independent supervision are enshrined in primary law for personal data processed not only by European Union institutions but also by Member States; these rules will be defined through the “ordinary legislative procedure”, which means that, as in the current co-decision procedure, the Parliament and the Council will be on equal footing and the Council will define its position by qualified majority.

The latter issue is particularly important in comparison with the current situation in the third pillar. So far, the specific decision-making procedure in this area – mere consultation of the European Parliament and unanimity in the Council – has profoundly affected the possibility of adopting a satisfactory general framework on data protection in the area of police and judicial cooperation. Even though the Commission launched a proposal already in October 2005, the quest for unanimity in the Council has resulted in a “lowest common denominator” approach which has been strongly criticized. Indeed, according to the European Parliament and the European data protection authorities, the result of the negotiations in the Council has been a dilution of the level of protection and lack of consistency with data protection rules already in place in the first pillar.

Now, the Lisbon Treaty paves the way for different solutions: on the one hand a greater involvement of the European Parliament, even before the entry into force of the Treaty, could determine a swift adoption of an adequate general legal framework; otherwise, the new legal basis provided by the Treaty could justify a broadening of the scope of the current data protection instruments (by amending, in particular, Directive 95/46), so as to extend their applicability to other areas of activities of the European Union.

Specificities of data processing in the areas of Common Foreign and Security Policy and of Police and Judicial Cooperation

The extension of the scope of the data protection legal instruments should however carefully take into account the specific provisions laid down by the new Article 39 of the Union Treaty as well as the declarations annexed to the Treaty, relating to common foreign and security policy, national security, and police and judicial cooperation.

Indeed, Article 39 of the Union Treaty derogates from paragraph 2 of the above mentioned Article 16, by establishing that specific rules on the protection of personal data processed by Member States in the area of Common Foreign and Security Policy will be laid down by the Council and that also in this case their application shall be subject to the control of independent authorities.

The subjective right to the protection of personal data laid down by Article 16, paragraph 1, will still apply in this area, but the procedure for the adoption of the specific rules will not involve the European Parliament. However, since Article 39 establishes derogation only with regard to processing of personal data by Member States, the general provision of Article 16 seems to remain fully applicable – including the involvement of the European Parliament – in the case of processing of personal data by European Union institutions.

This is particularly important since the Council and the Commission play a crucial role in managing the so called “terrorists blacklists”, lists of individuals and organizations whose assets are frozen because of their presumed connection with terrorist organizations, on the basis of information originating either from the United Nations or from Member States. Recently, the Court of Justice has annulled some of these listings on the basis of lack of compliance with basic procedural rights, such as the right to be informed about the reasons for inclusion in the list or the right to an independent review of the decision (cases *OMPI* and *Sison*).

In this context, the future definition of data protection rules and independent supervision also in the area of Common and Foreign Security Policy will undoubtedly enhance the quality and legitimacy of the Union's action in this area.

As for national security and police and judicial cooperation, the final Act of the Lisbon summit contains two specific declarations of the intergovernmental conference.

The first one (number 20) states that whenever data protection rules may have direct implications for national security, the specific characteristics of the issue should be duly taken into account. It also points out that current legislation, and in particular Directive 95/46, already lays down specific rules to this effect. This declaration actually does not seem to add much to the current legal framework, in which exceptions for public interests and national security are already possible.

The second one (number 21) recognizes that the specificities of judicial and police cooperation may justify specific data protection rules, to be adopted pursuant to Article 16 of the Treaty on the Functioning of the Union. This declaration basically calls for the adoption of certain sector-specific rules in this area.

In this context, it should be highlighted that, even if declarations are not binding, they have a strong political value and are bound to influence the interpretation of the new Treaty provisions on data protection and the development of the legislative instruments based on them.

The value of the Charter of Fundamental Rights and the European Convention of Human Rights.

A binding value is instead finally recognized by the Treaty to the Charter of Fundamental Rights. For political reasons, the Charter, formally proclaimed in Strasbourg on 12 December, is not part of the Treaty, but Article 6 of the European Union Treaty clearly states that it has the same legal value of the Treaties.

Therefore, its Article 8 on the protection of personal data will be in a position to play a role which goes far beyond the formal and symbolic proclamation as a fundamental right. In this perspective, firstly Article 8 confirms the broad scope of this right, to be respected throughout the whole range of activities of the European Union, under the supervision of independent authorities. Secondly, and more importantly, it gives a substantive contribution in spelling out its essential elements. In particular, paragraph 2 explicitly reaffirms that personal data must be processed fairly for specified purposes and on the basis of consent or some other legitimate basis laid down by law. Furthermore, it lays down the right of access and of rectification of one's personal data.

Therefore, these elements are explicitly recognized as crucial core values of the fundamental right to the protection of personal data. As such, possible limitations to their exercise shall be allowed only insofar as they are necessary to pursue a public interest, shall be laid down by law and shall in any case respect the essence of these rights (see Article 52 of the Charter). Furthermore, since Article 8 is sufficiently clear and precisely stated, and is unconditional in conferring a specific right for the citizens, it will have direct effect, i.e. the citizens will be able to enforce these rights before national courts (and data protection authorities) even in absence of specific implementing measures. This may happen, for example, in those areas falling outside the scope of national or Community data protection laws.

Another basic guarantee, reaffirmed by Article 8 of the Charter is the supervision by an independent authority. The use of the singular ("authority") rather than the plural ("authorities", used in the other Treaty provisions) does not seem to affect the possibility that the supervision might be carried out by more authorities, at European, national or sub-national level. The essential element is the independence, which should be a structural element of any single data protection authority. The Lisbon Treaty therefore confirms that ensuring independence (and, consequently, sufficient resources) for the supervisory authorities, at whatever level they may operate, is one of the main objectives and challenges for the future of data protection. In this regard, it is significant that the European Commission has recently made important steps in infringement procedures against Germany and Austria, alleging a lack of structural independence of certain sub-national data protection authorities.

The new version of Article 6, paragraph 2, of the European Union Treaty also grants the Union the competence (and the obligation) to accede to the European Convention of Human Rights. The modalities and conditions of this accession are further detailed in other provisions of the Lisbon Treaty (Article 218 of the Treaty on the Functioning of the Union and Protocol number 5). This accession will not only add substance to the protection of fundamental rights within the Union, but will also have great importance from an institutional point of view. European Union institutions

(including the Court of Justice) will be bound to comply with the provisions of the ECHR and their acts will be subject – according to modalities to be negotiated and agreed - to the scrutiny of the Strasbourg Court of Human Rights.

Furthermore, Article 6, paragraph 3, confirms that fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.

From a data protection perspective, this “double tie” with the ECHR is important in particular because it confirms the relevance of Article 8 ECHR and the case law of the Strasbourg Court within the European Union legal framework, while enhancing the institutional and procedural guarantees.

In conclusion, neither the provisions of the Charter nor the accession to the European Convention of Human Rights are meant to have as effect an extension of the competences of the European Union. However, the fundamental rights laid down by these two instruments should be fully complied with both by European Union institutions and by Member States acting within the scope of European Union law (see Article 51 of the Charter).

Against this background, the Protocol on the application of the Charter to Poland and United Kingdom is unlikely to have, beside its symbolic political value, any appreciable legal consequences on the full recognition in these countries of the right to the protection of personal data.

New developments in the Area of Freedom, Security and Justice

The Lisbon Treaty also contains some important developments in the field of police and judicial cooperation, which are likely to have considerable impact on data protection. Indeed, as the experience of last years has shown, the creation of an Area of Freedom, Security and Justice entails increasing exchanges of personal data between authorities of different Member States, as well as with third countries and international organizations.

In this regard, the Lisbon Treaty makes some big steps forward: extends the qualified majority voting in the Council and grants the European Parliament the role of full co-legislator also in this area, through the extension of the now called “ordinary legislative procedure”; extends the so far limited competences of the Court of Justice; allows the Commission to start infringement procedures also in this area, thus ensuring better and more uniform implementation of European Union legislation; establishes that the assent of the European Parliament will be necessary for the conclusion of international agreements in the field of police and judicial cooperation.

The Protocol on transitional provisions (number 10) mitigates and delays the effects of the remarkable advancements through some transitional arrangements that can be summarized as follows: the legal effects of all acts adopted before the entry into force of the Lisbon Treaty will be preserved, until these acts are repealed, annulled or amended; the extended competences of the Court of Justice and the possibility for the Commission to launch infringement procedures will not apply to these acts, until they are amended or 5 years from the entry into force of the Treaty have elapsed.

The “normalization” of the decision making process and of the judicial review in the area of police and judicial cooperation will bring, a least in the medium run, positive effects with regard to the quality and the consistency of the legal framework in this area, including the crucial aspects relating to the protection of personal data. General data protection frameworks, as well as specific tailored rules that may be necessary for specific exchanges of data, will benefit from the full involvement of all institutional actors. The European Parliament will be in a position to considerably influence those international agreements involving exchanges of personal data with third countries and even to block them, for example in case they fail to ensure an adequate level of protection.

A last remark concerns the various Protocols on the position of the United Kingdom, Ireland and Denmark allowing, to different degrees, the possibility to opt-out from all or part of the legal instruments adopted in the area of police and judicial cooperation. Those Member States that opt-out from a specific form of cooperation will not be bound by the corresponding norms on data

protection. Only the practice will show the concrete effects of these possible opt-outs. However, it is reasonable to assume that, while these provisions could limit the effects of certain sector-specific rules, they should not be interpreted in a way that would fully exclude the application of general frameworks and basic principles of data protection. In this context, it is interesting to highlight the judgement of 18 December 2007, in which the Court of Justice upheld the Council refusal to allow United Kingdom to participate "à la carte" to certain provisions of the Schengen *acquis*.

Taking Data Protection into the 21st century?

The Lisbon Treaty, which has been described as the Treaty that takes Europe into the 21st century, can be said to represent at the same time a success and a challenge for data protection.

On the one hand its provisions are not revolutionary, but mark an important and visible consolidation in the European Union primary law of the data protection *acquis* developed in Europe over the last 27 years. In this perspective, the Lisbon Treaty pinpoints some crucial elements of the fundamental right to the protection of personal data, within the context of the increased protection of fundamental rights. In addition, the need for independent supervision is solidly carved in primary law.

On the other hand, it develops instruments for a stronger and more homogeneous data protection across the different activities of the European Union, with a greater involvement of the European Parliament, also with regard to international agreements. When it comes to finding a delicate balance between conflicting values in crucial areas such as police and judicial cooperation, political negotiations are now likely to play a more important role than litigation before the Court of Justice.

In this perspective, the new tools laid down by the Lisbon Treaty represent a challenge for data protection in the 21st century. Many horizons are possible with a view to build a data protection legal framework which is comprehensive and general but at the same time able to accommodate the specificities of certain areas. Many efforts are required to address the growing demand for security and the immense possibilities offered by new technologies. Dialogue and communication, also at global level, are needed to involve citizens and explain them the important political choices made about their privacy.

Therefore, the new legal framework of the European Union is a challenge for the legislator, but also for data protection authorities, that will be called not only to supervise rules having an increasing degree of complexity but also to advise the legislator in making difficult and important choices in new fields of activities.