Data protection in the EU - Challanges Ahead

Reding Vivane

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

AUTHOR

Reding Vivane

CITATION SUGGESTION

R. Vivane, "Data protection in the EU - Challanges Ahead", 2010, Vol. 5(1), eucrim, pp25–1. DOI: https://doi.org/10.30709/eucrim-2010-001

Published in
2010, Vol. 5(1) eucrim pp 25 – 1
ISSN: 1862-6947
https://eucrim.eu

Introduction

The processing of personal data has become an inherent part of the daily life of Europeans, for example when booking a flight ticket, transferring money, applying for a job, or just using the Internet for private purposes. Nobody wants to miss out on the advantages of modern technologies. Sometimes individuals provide their personal data simply because they choose to do so. But sometimes data is collected without consent and often without the knowledge of the individuals concerned. The protection of personal data is becoming more and more relevant as technology develops and the possibilities increase to use and misuse information more efficiently.

Processing personal data also plays an increasing role in police and judicial cooperation: the lawful storage, exchange, and evaluation of information about a person can be an important instrument in ensuring public security.

The entry into force of the Lisbon Treaty[1] provides a much needed opportunity to reflect on the main challenges for the protection of personal data and on how the European Commission intends to address these challenges in the future.

The Protection of Personal Data at the European Level

The protection of personal data is one of the basic values in Europe, for the Member States of the EU and for the EU institutions.

The current protection of personal data in the Union is governed by Article 8 of the Charter of Fundamental Rights of the European Union ("EU Charter")[2] and specified in the general Data Protection Directive 95/46/EC[3] as well as complemented by Directive 2002/58/EC on privacy and electronic communications.[4] The processing by EU institutions and bodies is covered by

Data Protection Regulation (EC) No 45/2001.[5] Since 2008, the EU general framework for the protection of personal data in police and judicial cooperation in criminal matters is Framework Decision 2008/977/JHA[6].

The protection of personal data as a fundamental right

Article 8 of the EU Charter of Fundamental Rights enshrines the fundamental right of every individual to the protection of his/her personal data. Equally, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[7] guarantees the right to respect private and family life, which includes the right to protection of personal data.

Article 8 of the EU Charter defines the basic principles for data protection in an exemplary way. It reads as follows:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority."*

Unlike other countries, notably the US, EU legal rules on data protection do not discriminate between EU citizens and foreigners – the fundamental right to personal data protection is guaranteed to "every person" in Europe, citizens and non-citizens alike.

The *acquis* for the protection of personal data

In secondary law, data protection in the EU has been regulated since 1995. This EU legal framework for data protection – primarily Directive 95/46/EC on the protection of personal data – has also served as a much admired standard for third countries when regulating data protection. Its effect and impact, within and outside the EU, have been of utmost importance.

Directive 95/46/EC is the central piece of legislation on the protection of personal data in Europe. It set a milestone in the history of the protection of personal data as a fundamental right. The principles of the protection of the rights and freedoms of individuals, which are contained in this Directive, notably the right to privacy, give substance to and amplify those principles contained in Council of Europe Convention 108 of 28 January 1981 (and its additional protocol on transborder data flows and independent supervisory authorities, added in 2001 after implementation of the Directive).[8]

Directive 95/46/EC enshrines two of the oldest aims of the European integration project: the achievement of an Internal Market (in this case, the free movement of personal data) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important. Legislation at the EU level was justified because differences in the way that Member States approached this issue impeded the free flow of personal data between the Member States.

The Directive applies to and has been implemented by all 27 EU Member States as well as by the three EEA/EFTA States: Iceland, Liechtenstein, and Norway. Switzerland has also implemented the Directive for the Schengen area. In line with the Copenhagen criteria, all candidate countries are committed to transposing Directive 95/46/EC by the time of accession.

The Directive applies to both the public and private sectors. It develops and specifies data protection principles in order to achieve harmonisation throughout the EU. The Directive stipulates general rules on the lawfulness of personal data processing and the rights of the people whose data are processed ("data subjects"). The Directive also sets out that at least one independent supervisory authority in each Member State shall be responsible for monitoring its implementation. In particular, the Directive regulates transfers of personal data to third countries: in general, personal data cannot be exchanged with a third country unless the latter provides guarantees for an adequate level of protection.

In the area of police and judicial cooperation in criminal matters, the current data protection framework in the EU can only be described as a patchwork, as several instruments exist with specific data protection regimes or with data protection clauses. The legal provisions on Europol,[9] Eurojust,[10] the Schengen Information System,[11] and those contained in the "Prüm" Council decision[12] are just examples of such sector-specific regimes, the creation of different rights and obligations for Member States and individuals, and the setting up of several data protection supervisory authorities.[13]

Since 2008, Framework Decision 2008/977/JHA has aimed at creating an EU general legislative framework for the protection of personal data in police and judicial cooperation in criminal matters. Implementation of Framework Decision 2008/977/JHA is due for November 2010. It fully applies to the UK and Ireland, as well as Iceland, Norway, and Switzerland, as it is a development of the Schengen acquis. It does not, however, replace the rules applicable to Europol, Eurojust, Schengen, and the Customs Information System and also does not create a single independent supervisory authority.

Critics, such as the European Data Protection Supervisor (EDPS), point out that, in direct comparison with Directive 95/46/EC, this particular Framework Decision provides *inter alia* only for minimum standards and has a scope limited to the processing of personal data transmitted or made available between Member States.[14]

In view of such shortcomings, the European Parliament explicitly called for a timely revision of Council Framework Decision 2008/977/JHA in its Resolution on the Stockholm programme.[15]

The Treaty of Lisbon

The Lisbon Treaty led to a fundamental change in the system for the protection of personal data in the EU:

First, with the entry into force of the Lisbon Treaty on 1 December 2009, by virtue of the first subparagraph of Article 6(1) of the Treaty on European Union (TEU), the EU Charter of Fundamental Rights has the same legal value as the Treaties.

Second, the Lisbon Treaty newly introduced Article 16 Treaty on the Functioning of the European Union (TFEU) to become the sole legal basis for the protection of personal data in the EU. On this basis, the European Parliament and the Council will – as co-legislators – be able to adopt rules with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law as well as rules relating to the free movement of such data. This is without prejudice to the specific rules for the protection of personal data laid down in Article 39 TEU for Common Foreign and Security Policy (CFSP) by Member States.

Article 16 paragraph 2 TFEU applies to all forms of data processing in the private and in the public sector and particularly includes the area of police and judicial cooperation in criminal matters, which was previously not the case. However, Declaration 21, attached to the Lisbon Treaty, states that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU "may prove necessary because of the specific nature of these fields."

Challenges for the Protection of Personal Data

The main findings of the Eurobarometer Survey of 2008[16] show that a majority of EU citizens have concerns about data protection issues: two-thirds of survey participants said they were concerned as to whether organisations in possession of their personal data handled this data appropriately (64%). Most European Internet users feel uneasy when transmitting their personal data over the Internet: 82% of Internet users believe that data transmission over the Web is not sufficiently secure.

In very general terms, the main causes for this uneasiness result from three trends, which certainly pose a challenge for the protection of personal data in the future: the astounding capabilities of modern technologies, the increased globalisation of data flows, and access to personal data by law enforcement authorities that is greater than ever.

Modern technologies

The growth in new technologies, mobile Internet devices, and web-user generated content is increasingly pushing individuals to the fore when it comes to the "management" of their personal data, requiring a shift in focus on the part of policy makers.

Social networking sites, like Facebook, MySpace, StudiVZ or Twitter, to name but a few, have become extremely popular on a global scale, particularly among young people. Millions of people use these sites everyday to keep in touch with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet. All of this is based on personal data processing. And important revenue is being generated by tracking users on the Internet with "behavioural advertising."

Globalised data flows

Globalisation has seen an increasing role of third countries relating to data protection and has also led to a steady increase in the processing of the personal data of Europeans by companies and public authorities outside the European Union.

For example, in a recent move, ten privacy commissioners from the national data protection authorities of Canada, France, Germany, Ireland, Israel, Italy, New Zealand, the Netherlands, Spain, and the UK addressed a joint letter to Google's CEO Eric Schmidt complaining that the company was overlooking privacy values and legislation when rolling out products. These regulators rightly want Mountain View[17] to adopt a set of data protection principles that include collecting and processing only the minimum amount of personal data needed for a Google product or service, providing better disclosure to its users, and creating privacy-protective default settings.

Access to personal data by law enforcement authorities

In addition to the increasing technical possibilities, the growing appetite for personal data for reasons of public interest, in particular for public security matters, is also an important challenge for data protection. The collection and processing of personal information can be very valuable in order to secure important and legitimate public and private interests – if done in a lawful way.

A practical example is the use of body scanners for passenger screening at airports: before a new technology can be accepted as a regular and standardised method for passenger screening in all European airports, a careful assessment in regard to privacy and the protection of personal data is necessary. The assessment is complex, but the determinant criteria are clear: the use of body scanners must be lawful, their use and purposes laid down by law, the collected data must be necessary for passenger screening in order to improve security, no less intrusive alternatives regarding the privacy of passengers should be available that could achieve the same results, and there must be a sound relationship between the necessity and effectiveness of body scanners on the one hand and their impact on privacy on the other.

Due to the increase in transborder and transatlantic data processing as a means of preventing, detecting, investigating, and prosecuting criminal and terrorist acts, an effective protection of personal data is required, in particular, in the field of police and judicial cooperation, both within the European Union and when cooperating with international partners. The controversial discussions about these information exchanges have fuelled several specific agreements in the past between the USA and the EU, thus leading to the inclusion of provisions on the protection of personal data.[18]

The European Commission is Acting

The question has thus legitimately arisen whether today's legal framework at the EU level is still fully equipped to deal with all these new challenges – a question coming first and foremost from within the Commission itself.

Listening to stakeholders

In order to hear from the various stakeholders, the European Commission held a public consultation on the future of privacy, which featured – as part of a broader initiative – a review of the current European data protection framework in its entirety. This public consultation was intended to reach a broad sampling of stakeholders, based on three very open questions, leaving them as much leeway as possible in identifying new challenges, signalling out areas that would need improvement, and making suggestions on how a future legal framework could better tackle certain problems.

The preliminary results have shown that the current legal framework – in particular Directive 95/46/EC – is generally rooted in very strong data protection principles, still regarded as sound, and aptly equipped to regulate data protection throughout the European Union. The technological neutrality of the Directive has also been widely celebrated and there is consensus on not stepping away from this paradigm. It is mainly the application of these principles in practice that causes problems and where action is needed.

The main challenges identified in the submitted contributions of the above-mentioned public consultation are the divergences between Member States' legislations implementing the Directive – which potentially disrupt the Internal Market –, the need for administrative simplification in dealing with Data Protection Authorities (e.g., regarding notification requirements), the need to update definitions and concepts in light of new technologies, and the need to better regulate international data transfers with third countries.

We also obtained confirmation that our citizens are increasingly worrying about what they perceive as a growing demand by public authorities to gather and request personal data, both inside and outside the EU, either directly or via private actors. Citizens are also concerned with whether they are still able to exercise their data protection rights once their data leaves the European Union.

The joint opinion of the Working Party established by Article 29 of the Directive together with the Working Party on Police and Judicial Cooperation[19] has made a notable contribution. The national data protection authorities identified key issues that have to be addressed in order to modernise and streamline the data protection framework, suggesting ways to better tackle these issues in the future. They see a further need to include the fundamental principles of data protection into one comprehensive legal framework at the EU level, which also applies to police and judicial cooperation in criminal matters.

An Action Plan for the next five years

With the entry into force of the Lisbon Treaty on 1 December 2009, the EU now has the tools to bring a new balance to policies in order to strengthen the rights and freedoms of Europeans. The protection of the fundamental right to data protection has been set as one important strategic initiative in the work programme of the Commission for 2010.[20]

In December 2009, European leaders endorsed the Stockholm Programme.[21] It sets out objectives aiming at creating a genuine European area of freedom, security and justice in the next five years. In April 2010, the European Commission turned these political objectives into an Action Plan for 2010-2014.[22] In the justice, fundamental rights and citizenship area, the plan includes proposals to improve data protection for data subjects in all EU policies – including law enforcement and crime prevention – and in relations with international partners.

The Commission will tackle the challenges for the protection of personal data by means of two concrete actions:

Modernising Data Protection Directive 95/46/EC

Firstly, by the end of 2010, Data Protection Directive 95/46/EC will be modernised in response to the latest technological developments, so that the EU *acquis* continues to guarantee a high level of protection of individuals with regard to the processing of personal data. Also, the Commission aims at achieving a consistent, coherent, and effective legal implementation and application of the fundamental right to protection of personal data in all areas of the Union's activities.

This is likely to result in an increased harmonization of data protection legislation in Member States by clarifying the application of some key rules and principles of data protection (such as applicable law, consent, and transparency), introducing some additional principles (such as "privacy by design"), strengthening the effectiveness of the system by modernising existing arrangements (e.g., limiting bureaucratic burdens), and – most importantly – by extending the fundamental principles of data protection into one comprehensive EU legal framework, which also applies to police and judicial cooperation in criminal matters.

Therefore, the rules of Framework Decision 2008/977/JHA should be improved and integrated into a new coherent legal framework based on Directive 95/46/EC, while taking into account the specificities of police cooperation and judicial cooperation in criminal matters where necessary. Where appropriate, this will also mean adapting and/or repealing existing data protection clauses or provisions in other former third pillar legislation. This exercise will, in the long term, also affect the current regimes for Europol and Eurojust. It will also affect other instruments devised in the former third pillar. Particular attention will have to be paid as regards the independent supervision of data protection processing where there are currently different supervisory authorities.

A data protection agreement between the EU and the US

Secondly, the Commission will present a negotiation text by summer 2010 for an "umbrella" data protection agreement between the EU and the US. As stated by the European Council in the Stockholm Programme, the EU must be a driving force behind the development and promotion of international standards for the protection of personal data.

This data protection agreement should ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular the right to protection of personal data, and be fully in line with the EU Charter of Fundamental Rights as well as the Lisbon Treaty. It should only apply when personal data is transferred and processed by competent public authorities of the EU and its Member States and the US exclusively for the purpose of preventing, investigating, detecting, or prosecuting crime, including terrorism, within the framework of police cooperation and judicial cooperation in criminal matters, as these are the areas which have sparked controversy in the past.

The agreement should provide legal certainty and fill the current "protection gap" with a set of clearly defined data protection rights for European data subjects, such as the possibility to file complaints about unlawful processing of personal data. Data protection complaints by European citizens should be handled in the same manner as those filed by American citizens in US courts, which is not the case today.

Conclusion

There are many challenges ahead for the protection of personal data. Our citizens will now expect action and concrete results from Europe. The Lisbon Treaty and the adoption of the Stockholm action plan are ideally timed to turn our policies into practical results.

I have repeatedly stressed that I intend to use all of the powers given by the Lisbon Treaty to effectively improve the European rules on the protection of personal data, so that it may fully reflect the status of fundamental rights contained therein in daily life.

European personal data should be protected according to European data protection standards. This also means that, for any processing of personal data, there must be strong and effective supervision of these standards by independent supervisory authorities and, ultimately, the courts of justice. European data subjects must enjoy the protection of the same data protection principles from the North Cape to the tip of Malta Island, from the shores of the Atlantic to the Eastern Mediterranean Sea, and wherever their data are processed across other parts of the globe.

I am determined to work in this direction. I also have no doubt that the European Union will continue to fulfil its role as a key player in setting the standards for personal data protection, as it has done for the past 15 years.

---

1. For the consolidated versions of the Treaty on European Union and of the Treaty on the Functioning of the European Union, together with the annexes and protocols thereto, as they result from the amendments introduced by the Treaty of Lisbon, see OJ 2010 C 83/1.↩
2. Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.↩
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ 1995 L 281/31.↩
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 , 31/07/2002 pp. 0037 – 0047.↩
5. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ 2001 L 8/1.↩
6. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350/60.↩
7. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4.11.1950 (European Treaty Series - No. 5; http://conventions.coe.int).↩
8. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108; regarding supervisory authorities and transborder data flows, see also Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 181, available at: www.coe.int.↩
9. Europol Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ 2009 L 121/37.↩
10. Eurojust Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L 138/14.↩
11. Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders; OJ 2000 L 239/19.↩
12. Council Decision 2008/615/JHA, of 23 June 2008, on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210/1.↩
13. See for data protection authorities at the national level, the EDPS and the Joint Supervisory Board for Europol, Customs, Schengen (with a common secretariat), in addition to Eurojust and its Supervisory Body.↩
14. Cf. second and third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters; OJ 2007 C 91/2; OJ 2007 C 139/01.↩
15. P7_TA-PROV(2009)0090.↩
16. Data Protection in the European Union-Citizens' perceptions- Analytical report, Flash Eurobarometer Series 225, January 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf; http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf.↩
17. Mountain View is the seat of the headquarter of Google Inc., (1600 Amphitheatre Parkway, Mountain View, CA 94043, United States).↩
18. See, for example, the US-Europol cooperation agreement: http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf; US-Eurojust agreement: http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_co-operation_agreement.pdf ; 2007 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ 2007 L 204 /16.↩
19. Joint contribution of Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 December 2009 (02356/09/EN WP). http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.↩
20. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Commission Work Programme 2010 (COM (2010) 135, http://ec.europa.eu/atwork/programmes/index_en.htm.)↩
21. "The Stockholm Programme – An open and secure Europe serving and protecting the citizens", Council document 17024/09.↩
22. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Delivering an area of freedom, security and justice for Europe's citizens; Action Plan Implementing the Stockholm Programme COM(2010)171 final.↩

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union