P7_TA(2011)0323

Personal data protection in the European Union

European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI))

The European Parliament,

– having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

– having regard to the Charter of Fundamental Rights of the European Union, in particular its Articles 7 and 8, and to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), in particular Article 8 on the protection of private and family life and Article 13 on effective remedy,

– having regard to 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[1],

– having regard to 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[2],

– having regard to 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[3],

– having regard to 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)[4],

– having regard to Council of Europe Convention 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data that Directive 95/46/EC develops and the additional protocol thereto of 8 November 2001 regarding supervisory authorities and transborder data flows, and to the Committee of Ministers' recommendations to Member States, in particular Recommendation No. R (87) 15 regulating the use of personal data in the police sector and Recommendation CM/Rec. (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling,

– having regard to the Guidelines for the regulation of computerised personal data files issued by the United Nations General Assembly in 1990,

---

1 OJ L 281, 23.11.1995, p. 31.
2 OJ L 350, 30.12.2008, p. 60.
3 OJ L 8, 12.1.2001, p. 1.
4 OJ L 201, 31.7.2002, p. 37.

– having regard to the Commission communication to Parliament, the Council, the Economic and Social Committee and the Committee of the Regions entitled 'A comprehensive approach on personal data protection in the European Union' (COM(2010)0609),

– having regard to the Council conclusions concerning the Commission communication entitled 'A comprehensive approach on personal data protection in the European Union'[1],

– having regard to the opinion of the European Data Protection Supervisor (EDPS) of 14 January 2011 concerning the Commission communication entitled 'A comprehensive approach on personal data protection in the European Union',

– having regard to the joint contribution by the 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 entitled 'The Future of Privacy'[2],

– having regard to Opinion 8/2010 of the Article 29 Data Protection Working Party concerning applicable law[3],

– having regard to its previous resolutions on data protection and its resolution on the Stockholm Programme[4],

– having regard to Rule 48 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Industry, Research and Energy, the Committee on the Internal Market and Consumer Protection, the Committee on Culture and Education and the Committee on Legal Affairs (A7-0244/2011),

A. whereas the Data Protection Directive 95/46/EC and the EU Telecoms Package Directive 2009/140/EC make the free flow of personal data within the internal market possible,

B. whereas data protection legislation in the EU, the Member States and beyond has developed a legal tradition that must be maintained and further elaborated,

C. whereas the core principle of the 95/46/EC Data Protection Directive remain valid, but different approaches in Member States' implementation and enforcement thereof have been observed; whereas the EU must equip itself – after a thorough impact assessment – with a comprehensive, coherent, modern, high-level framework able to protect effectively

---

1 3071st Justice and Home Affairs Council meeting, Brussels, 24 and 25 February 2011, available at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

2 02356/09/EN WP 168.

3 0836/10/EN WP 179.

4 For example: European Parliament position of 23 September 2008 on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ C 8 E , 14.1.2010, p. 138); European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the internet (OJ C 117 E , 6.5.2010, p. 206); European Parliament resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme (OJ C 285 E , 21.10.2010, p. 12).

individuals' fundamental rights, in particular privacy, with regard to any processing of personal data of individuals within and beyond the EU in all circumstances, in order to face the numerous challenges facing data protection, such as those caused by globalisation, technological development, enhanced online activity, uses related to more and more activities, and security concerns (e.g. the fight against terrorism); whereas a data protection framework such as this can increase legal certainty, keep the administrative burden to a minimum, provide a level playing field for economic operators, boost the digital single market and trigger trust in the behaviour of data controllers and enforcement authorities,

D. whereas violations of data protection provisions can lead to serious risks for the fundamental rights of individuals and the values of the Member States, so that the Union and the Member States must take effective measures against such violations; whereas such violations lead to a lack of trust on the part of individuals that will weaken expedient use of the new technologies, and whereas misuse and abuse of personal data should therefore be punishable by appropriate, severe and dissuasive sanctions, including criminal sanctions,

E. whereas other relevant fundamental rights enshrined in the Charter and other objectives set out in the EU Treaties, such as the right to freedom of expression and information and the principle of transparency, must be fully taken into account when ensuring the fundamental right to protection of personal data,

F. whereas the new legal basis set out in Article 16 TFEU and the recognition in Article 8 of the Charter of Fundamental Rights of the right to protection of personal data and in Article 7 thereof of the right to respect for private and family life as an autonomous rights fully necessitate and support a comprehensive approach to data protection in all fields in which personal data are processed, including the field of police and judicial cooperation in criminal matters, the field of Common Foreign and Security Policy (CFSP) without prejudice to the specific rules laid down in Article 39 TEU, and the field of data processing by EU institutions and bodies,

G. whereas it is of the utmost importance that a series of key elements is taken into account when legislative solutions are being considered, consisting in effective protection given under all circumstances, independently of political preferences within a certain time frame; whereas the framework must be stable over a long period, and limitations on the exercise of the right, where and if needed, must be exceptional, in accordance with the law, strictly necessary and proportionate, and must never affect the essential elements of the right itself,

H. whereas the collection, analysis, exchange and misuse of data and the risk of 'profiling', stimulated by technical developments, have reached unprecedented dimensions and consequently necessitate strong data protection rules, such as applicable law and the definition of the responsibilities of all interested parties in terms of the implementation of EU data protection legislation; whereas loyalty cards (club cards, discount cards, advantage cards etc.) are being used more and more frequently by companies and in commerce, and are, or can be, used for customer profiling,

I. whereas citizens do not shop online with the same security as they do offline, owing to fears of identity theft and lack of transparency as to how their personal information will be processed and used,

J. whereas technology is increasingly making it possible to create, send, process and store personal data anywhere and at any time in many different forms, and whereas, against this

background, it is crucially important that data subjects retain effective control over their own data,

K. whereas the fundamental rights to data protection and privacy include the protection of persons from possible surveillance and abuse of their data by the state itself, as well as by private entities,

L. whereas privacy and security are possible and are both of key importance for citizens, so that there is no need to chose between being free and being safe,

M. whereas children deserve specific protection, as they may be less aware of risks, consequences, safeguards and rights in relation to the processing of personal data; whereas young people divulge personal data on social networking sites which are spreading rapidly on the internet,

N. whereas effective control by the data subject and by national data protection authorities requires transparent behaviour on the part of data controllers,

O. whereas not all data controllers are online businesses and thus new data protection rules must cover both the online and the offline environment, while taking possible differences between them into account,

P. whereas national data protection authorities are subject to widely diverging rules in the 27 Member States, particularly with regard to their status, resources and powers,

Q. whereas a strong European and international data protection regime is the necessary foundation for the flow of personal data across borders, and whereas current differences in data protection legislation and enforcement are affecting the protection of fundamental rights and individual freedoms, legal security and clarity in contractual relations, the development of e-commerce and e-business, consumer trust in the system, cross-border transactions, the global economy and the single European market; whereas, in this context, the exchange of data is of importance in enabling and ensuring public security at national and international level; whereas necessity, proportionality, purpose limitation, oversight and adequacy are preconditions for exchange,

R. whereas current rules and conditions governing the transfer of personal data from EU to third countries have lead to different approaches and practices in various Member States; whereas it is imperative that data subjects' rights are fully enforced in third countries where personal data are transferred and processed,

Fully engaging with a comprehensive approach

1. Strongly welcomes and supports the Commission communication entitled 'A comprehensive approach on personal data protection in the European Union' and its focus on strengthening existing arrangements, putting forward new principles and mechanisms and ensuring coherence and high standards of data protection in the new setting offered by the entry into force of the Lisbon Treaty (Article 16 TFEU) and the now binding Charter of Fundamental Rights, particularly its Article 8;

2. Emphasises that the standards and principles set out in Directive 95/46/EC represent an ideal starting point and should be further elaborated, extended and enforced, as part of a

modern data protection law;

3. Underlines the importance of Article 9 of Directive 95/46/EC, which obliges Member States to provide for exemptions from data protection rules when personal data are used solely for journalistic purposes or the purpose of artistic or literary expression; in this context calls on the Commission to ensure that these exemptions are maintained and that every effort is made to evaluate the need for developing these exceptions further in the light of any new provisions in order to protect freedom of the press;

4. Stresses that the technologically neutral approach of Directive 95/46/EC should be maintained as a principle of a new framework;

5. Recognises that technological developments have on the one hand created new threats to the protection of personal data and on the other led to a vast increase in the use of information technologies for everyday and normally harmless purposes, and that these developments mean that a thorough evaluation of the current data protection rules is required in order to ensure that (i) the rules still provide a high level of protection, (ii) the rules still strike a fair balance between the right to protection of personal data and the right to freedom of speech and information, and (iii) the rules do not unnecessarily hinder everyday processing of personal data, which is typically harmless;

6. Considers it imperative to extend the application of the general data protection rules to the areas of police and judicial cooperation, including processing at domestic level, taking particular account of the questionable trend towards systematic re-use of private-sector personal data for law enforcement purposes, while also allowing, where strictly necessary and proportionate in a democratic society, for narrowly tailored and harmonised limitations to certain data protection rights of the individual;

7. Emphasises the need for the processing of personal data by institutions and bodies of the European Union, which is governed by Regulation (EC) No 45/2001, to be included within the scope of the new framework;

8. Recognises that additional, enhanced measures may be needed in order to specify how the general principles set up by the comprehensive framework apply to specific sectors' activities and data processing, as already done in the case of the e-Privacy Directive, but insists that such sector-specific rules should in no circumstances lower the level of protection provided by the framework legislation, but should strictly define exceptional, necessary, legitimate, narrowly tailored derogations to general data protection principles;

9. Calls on the Commission to ensure that the current revision of EU data protection legislation will provide for:

   – full harmonisation at the highest level providing legal certainty and a uniform high level standard of protection of individuals in all circumstances,

   – further clarification of the rules on applicable law with a view to delivering a uniform degree of protection for individuals irrespective of the geographical location of the data controller, also covering enforcement of data protection rules by authorities or in courts;

10. Takes the view that the revised data protection regime, while fully enforcing the rights to

privacy and data protection, should keep bureaucratic and financial burdens to a minimum and provide instruments enabling conglomerates perceived as single entities to act as such rather than as a multitude of separate undertakings; encourages the Commission to conduct impact assessments and carefully evaluate the costs of new measures;

Strengthening individuals' rights

11. Calls on the Commission to reinforce existing principles and elements such as transparency, data minimisation and purpose limitation, informed, prior and explicit consent, data breach notification and the data subjects' rights, as set out in Directive 95/46/EC, improving their implementation in Member States, particularly as regards the 'global online environment';

12. Underlines the fact that consent should be considered valid only when it is unambiguous, informed, freely given, specific and explicit, and that adequate mechanisms to record users' consent or revocation of consent must be implemented;

13. Points to the fact that voluntary consent cannot be assumed in the field of labour contracts;

14. Is concerned about the abuses stemming from online behavioural targeting and points out that, under the directive on privacy and electronic communications, the prior explicit consent of the person concerned is required for the display of cookies and for further monitoring of his or her web-browsing behaviour for the purpose of delivering personalised advertisements;

15. Fully supports the introduction of a general transparency principle, as well as the use of transparency-enhancing technologies and the development of standard privacy notices enabling individuals to exercise control over their own data; stresses that information on data processing must be provided in clear, plain language and in a manner that is easily understandable and accessible;

16. Underlines, furthermore, the importance of improving the means of exercising, and awareness of, the rights of access, of rectification, of erasure and blocking of data, of clarifying in detail and codifying the 'right to be forgotten'[1] and of enabling data portability[2], while ensuring that full technical and organisational feasibility is developed and in place to allow for the exercise of those rights; stresses that individuals need sufficient control of their online data to enable them to use the internet responsibly;

17. Stresses that citizens must be able to exercise their data rights free of charge; calls on companies to refrain from any attempts to add unneeded barriers to the right of access, or to amend or delete personal data; stresses that data subjects must be put in a position to know at any time what data have been stored, by whom, when, for what purpose and for what time period, and how they are being processed; emphasises that data subjects must be able to have data deleted, corrected or blocked in an unbureaucratic way and that they must be informed of any misuse of data or data breach; demands also that data be disclosed at the

---

[1] There must be clear and precise identification of all the relevant elements underpinning this right.

[2] Portability of personal data will facilitate the smooth functioning of both the single market and the internet and its characteristic openness and interconnectivity.

request of the person concerned and deleted, at the latest, when the person requests it; underlines the need to communicate clearly to data subjects the level of data protection in third countries; emphasises that the right of access includes not only full access to processed data about oneself, including its source and recipients, but also intelligible information about the logic involved in any automatic processing; emphasises that the latter will become even more important with profiling and data-mining;

18. Points out that profiling is a major trend in the digital world, owing not least to the growing importance of social networks and integrated internet business models; calls on the Commission, therefore, to include provisions on profiling, while clearly defining the terms 'profile' and 'profiling';

19. Reiterates the need to enhance obligations of data controllers with regard to provision of information to data subjects, and welcomes the attention given by the Communication to awareness-raising activities directed at the general public and also, more specifically, at young people; emphasises the need for specific procedures to deal with vulnerable persons, in particular children and the elderly; encourages the various actors to undertake such awareness-raising activities, and supports the Commission's proposal to co-finance awareness-raising measures on data protection via the Union budget; calls for the efficient dissemination in each Member State of information concerning the rights and obligations of natural and legal persons regarding the collection, processing, storage and forwarding of personal data;

20. Points to the need to provide for specific forms of protection for vulnerable persons, especially children, for instance by requiring a high level of data protection to be used as the default setting and by taking appropriate specific measures to protect their personal data;

21. Stresses the importance of data protection legislation acknowledging the need to specifically protect children and minors – in the light, inter alia, of increased access for children to internet and digital content – and emphasises that media literacy must become part of formal education with a view to teaching children and minors how to act responsibly in the online environment; to this end, particular attention should be given to provisions on the collection and further processing of children's data, the reinforcement of the purpose limitation principle in relation to children's data and to how children's consent is sought, and on protection against behavioural advertising[1];

22. Supports further clarification and reinforcement of guarantees on the processing of sensitive data, and calls for reflection on the need to deal with new categories such as genetic and biometric data, especially in the context of technological (e.g. cloud computing) and societal developments;

23. Stresses that personal data concerning a user's professional situation which is given to their employer should not be published or forwarded to third parties without the prior permission of the person concerned;

Further advancing the internal market dimension and ensuring better enforcement of data protection rules

---

[1] Consideration could be given to an age threshold for children below which parental consent is sought and to age verification mechanisms.

24. Notes that data protection should play an ever greater role in the internal market, and stresses that effective protection of the right to privacy is essential to gaining individuals' confidence, which is needed in order to unlock the full growth potential of the digital single market; reminds the Commission that common principles and rules for both goods and services are a prerequisite for a single digital market, as services are an important part of the digital market;

25. Reiterates its call on the Commission to clarify the rules related to applicable law in the field of personal data protection;

26. Considers it essential to reinforce data controllers' obligations to ensure compliance with data protection legislation by having in place, inter alia, proactive mechanisms and procedures, and welcomes the other directions suggested by the Commission communication;

27. Recalls that in this context special attention must be paid to data controllers who are subject to professional secrecy obligations and that the building of special structures for data protection supervision should be considered in their case;

28. Welcomes and supports the Commission's consideration of the introduction of a principle of accountability, as it is of key importance in ensuring that data controllers act in accordance with their responsibility; at the same time calls on the Commission to carefully examine how such a principle could be implemented in practice and to assess the consequences thereof;

29. Welcomes the possibility of making the appointment of organisation data protection officers mandatory, as the experience of EU Member States which already have data protection officers shows that the concept has proved successful; points out, however, that this must be carefully assessed in the case of small and micro-enterprises with a view of avoiding excessive costs or burden upon them;

30. Also welcomes, in this context, the efforts being made to simplify and harmonise the current notification system;

31. Considers it essential to make Privacy Impact Assessments mandatory in order to identify privacy risks, foresee problems, and bring forward proactive solutions;

32. Considers it of utmost importance that data subjects' rights are enforceable; notes that class-action lawsuits could be introduced as a tool for individuals to collectively defend their data rights and seek reimbursement of damages resulting from a data breach; notes, however, that any such introduction must be subject to limits in order to avoid abuses; asks the Commission to clarify the relationship between this communication on data protection and the current public consultation on collective redress; calls therefore for a collective redress mechanism for breach of data protection rules to allow data subjects to get compensation for the damages suffered;

33. Highlights the need for proper harmonised enforcement across the EU; calls on the Commission to provide in its legislative proposal for severe and dissuasive sanctions, including criminal sanctions, for misuse and abuse of personal data;

34. Encourages the Commission to introduce a system of mandatory general personal data

breach notifications by extending it to sectors other than the telecommunications sector, while ensuring that (a) it does not become a routine alert for all sorts of breaches, but relates mainly to those that may impact negatively on the individual and (b) that all breaches without exception are logged and at the disposal of data protection or other appropriate authorities for inspection and evaluation, thus ensuring a level playing field and uniform protection for all individuals;

35. Sees in the concepts of 'privacy by design' and 'privacy by default' a strengthening of data protection, and supports their concrete application and further development as well as the need to promote the use of Privacy Enhancing Technologies; highlights the need for any implementation of 'privacy by design' to be based on sound and concrete criteria and definitions in order to protect individuals' right to privacy and data protection, and to ensure legal certainty, transparency, a level playing field and free movement; believes that 'privacy by design' should be based on the principle of data minimisation, meaning that all products, services and systems should be built in such a way as to collect, use and transmit only the personal data that are absolutely necessary to their functioning;

36. Notes that the development and broader use of cloud computing raises new challenges in terms of privacy and protection of personal data; calls, therefore, for clarification of the capacities of data controllers, data processors and hosts in order better to allocate the corresponding legal responsibilities and to ensure that data subjects know where their data are stored, who has access to their data, who decides on the use to which the personal data will be put, and what kind of back-up and recovery processes are in place;

37. Calls on the Commission, therefore, to take due account of data protection issues related to cloud computing when revising Directive 95/46/EC, and to ensure that data protection rules apply to all interested parties, including telecom operators and non telecom operators;

38. Calls on the Commission to ensure that all internet operators assume their responsibilities with regard to data protection, and urges advertising-space agencies and publishers to clearly inform internet users in advance about the collection of any data relating to them;

39. Welcomes the newly signed agreement on a Privacy and Data Protection Impact Assessment Framework for Radio Frequency Identification (RFID) applications, which seeks to ensure consumer privacy before RFID tags are introduced onto a given market;

40. Supports the efforts to further advance self-regulatory initiatives – such as codes of conduct – and the reflection on setting up voluntary EU certification schemes, as complementary steps to legislative measures, while maintaining that the EU data protection regime is based on legislation setting high-level guarantees; calls on the Commission to carry out an impact assessment of self-regulatory initiatives as tools for better enforcement of data protection rules;

41. Believes that any certification or seal scheme must be of guaranteed integrity and trustworthiness, technology-neutral, globally recognisable and affordable, so as not to create barriers to entry;

42. Is in favour of further clarifying, strengthening and harmonising the status and powers of national data protection authorities, and of exploring ways to ensure more consistent application of EU data protection rules across the internal market; emphasises, furthermore, the importance of ensuring coherence among the competencies of the EDPS, the national

data protection authorities and Working Party 29;

43. Emphasises in this context that the role and powers of the Article 29 Working Party should be strengthened in order to improve coordination and cooperation among the Data Protection Authorities of the Member States, especially in terms of the need to safeguard uniform application of data protection rules;

44. Calls on the Commission to clarify in the new legal framework the essential notion of independence of national data protection authorities in the sense of absence of any external influence[1]; stresses that the national data protection authorities should be given the necessary resources and be vested with harmonised investigative and sanctioning powers;

Strengthening the global dimension of data protection

45. Calls on the Commission to streamline and strengthen current procedures for international data transfers – legally binding agreements and binding corporate rules – and to define on the basis of the personal data protection principles referred to above the ambitious core EU data protection aspects to be used in international agreements; stresses that the provisions of EU personal data protection agreements with third countries should give European citizens the same level of personal data protection as that provided within the European Union;

46. Takes the view that the adequacy procedure of the Commission would benefit from further clarification and stricter implementation, enforcement and monitoring, and that the criteria and requirements for assessing the level of data protection in a third country or an international organisation should be better specified taking into account the new threats to privacy and personal data;

47. Calls on the Commission to assess carefully the effectiveness and correct application of the Safe Harbour Principles;

48. Welcomes the Commission's stance on reciprocity in levels of protection regarding data subjects whose data are exported to, or held in, third countries; calls on the Commission to take decisive steps towards enhanced regulatory cooperation with third countries with a view to clarifying the applicable rules and the convergence of EU and third-country data protection legislation; calls on the Commission to bring this forward as a priority agenda item in the relaunched Transatlantic Economic Council;

49. Supports the Commission's efforts to enhance cooperation with third countries and international organisations, including the United Nations, the Council of Europe and the OECD, as well as with standardisation organisations such as the European Committee for Standardisation (CEN), the International Organisation for Standardisation (ISO), the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF); encourages the development of international standards[2], while ensuring that there is coherence among initiatives for international standards and current revisions in the EU, the OECD and the Council of Europe;

---

1 In line with Article 16 TFEU and Article 8 of the Charter.

2 See the Madrid Declaration: Global Privacy Standards for a Global World October 2009 and Resolution on International Standards adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem 27-29 October 2010.

o

o o

50. Instructs its President to forward this resolution to the Council and the Commission.