EUROPEAN PARLIAMENT 2009 - 2014

Plenary sitting

A7-0244/2011

22.6.2011

REPORT

on a comprehensive approach on personal data protection in the European Union
(2011/2025(INI))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Axel Voss

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

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 8/10 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 1995/46/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 –

---

[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 legislative resolution 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 8E , 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 117E , 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 285E , 21.10.2010, p. 12).

with a comprehensive, coherent, modern, high-level framework able to protect effectively 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 and 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 duly justified, and must never affect the essential elements of the right itself[1],

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,

[1] See opinion of the EDPS (n7) [30].

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

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

portability[1], 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 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

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

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

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,

---

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

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 examination of possibilities for their concrete application and further development, as well as recognising 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

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

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[1], while ensuring that there is coherence among initiatives for international standards and current revisions in the EU, the OECD and the Council of Europe;

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

[1] 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.

11.5.2011

OPINION OF THE COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY

for the Committee on Civil Liberties, Justice and Home Affairs

on a comprehensive approach on personal data protection in the European Union
(2011/2025(INI))

Rapporteur: Giles Chichester

SUGGESTIONS

The Committee on Industry, Research and Energy calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Stresses that effective protection of the right to privacy is essential in order to ensure consumer confidence, which is required to unlock the full growth potential of the digital single market;

2. Believes that the digital single market requires common privacy protection arrangements coordinated at a European level, in order to encourage cross-border trade and prevent market distortions; stresses that a high level of protection for sensitive economic data (e.g. credit card numbers, addresses) is vital in terms of credibility and digital consumption;

3. 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;

4. Stresses that the Commission must consider all aspects, including verified need, legal certainty, reducing administrative burdens, maintaining a level playing field for operators, feasibility, cost and probable value with respect to data protection, in connection with any proposal;

5. Recognises that the Data Protection Directive (95/46/EC) has led to a fragmented legal framework due to different approaches in Member States' implementation and

enforcement and that new technological developments have led to new challenges in terms of data protection; agrees therefore that the need for a new legal framework has been confirmed;

6. Reminds the Commission that the effects of extending the categories of sensitive data must be thoroughly examined; maintains that the stricter criteria for dealing with sensitive data should not require numerous new legal authorisations to maintain necessary and desired data processing applications and that the list of sensitive data should be extended only in so far as to include all those data which are sensitive in (almost) all conceivable data processing situations, such as genetic data;

7. Calls on the Commission to amend Directive 95/46/EC not only so as to include additional categories of data (such as genetic data) but also so as to take account of the future development of 'new data', and to thoroughly revise the Directive in this field;

8. Reminds the Commission that not all data controllers are internet businesses; calls on the Commission to ensure that new data protection rules can be applied in both the online and the offline environments;

9. Calls on the Commission to further regulate the collection, sale and purchase of personal data by including this aspect in the scope of any new data protection rules; stresses that such data are not used for online purposes alone but also for direct postal marketing;

10. Invites the Commission, while maintaining a high level of data protection, to carefully consider the impact on SMEs, so as to ensure they are not disadvantaged, whether through unnecessary administrative burdens or through multiple notification requirements impeding their cross-border activities or other red tape; believes also that the volume and nature of data processed should be taken into consideration irrespective of the size of the controller;

11. Believes that the revision of the legal framework must ensure the flexibility required for the new framework to be able to meet future needs as technology develops; invites the Commission to assess any new provisions in accordance with the principle of proportionality and to ensure that they do not erect trade barriers, contravene the right to a fair trial or skew competition; stresses that any new principles must be designed to protect the rights of data subjects, be necessary for the achievement of that purpose and be sufficiently clear to ensure legal certainty and allow fair competition;

12. 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 therefore on the Commission to include provisions on profiling, while clearly defining the terms 'profile' and 'profiling';

13. Reminds the Commission that there is a need for a precise definition of the term 'right to be forgotten' that clearly identifies the relevant requirements and specifies against whom the right may be enforced;

14. Stresses that citizens must be able to exercise their data rights free of charge and without postal or other costs; calls on companies to refrain from any attempts to add unneeded

barriers to the right to view, amend or delete personal data;

15. Calls on the Commission to ensure that users of social networking sites can obtain a complete overview of the data which are held concerning themselves without this necessitating an unacceptable cost or effort;

16. Calls on the Commission to facilitate greater data portability on the internet while taking into account the business models of service providers, the existing technical systems and the legitimate interests of stakeholders; stresses that users need sufficient control of their online data for a sovereign and responsible use of the internet;

17. Believes that any certification or seal scheme could be based on a model such as EMAS and must in any event be of ensured integrity and trustworthiness; asks for any such scheme to include individual serial codes on certificates viewable by the public and checkable in a central public database;

18. Invites the Commission to encourage the strengthening of self-regulation initiatives, personal responsibility and the right to control one's own data, in particular as regards the internet;

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

20. Encourages all the bodies involved to work towards a common standard for determining when individuals may been deemed to have given their consent and towards a common 'age of consent' for data usage and transfer;

21. Welcomes the fact that the Commission is considering 'privacy by design' and recommends that any concrete implementation thereof be based on the existing EU model of the New Approach and the New Legislative Framework with respect to goods, in order to ensure free movement of products and services conforming to harmonised privacy and data protection requirements; highlights the need for any implementation thereof to be based on sound and concrete criteria and definitions in order to ensure users' right to privacy and data protection, 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 absolutely necessary for them to function;

22. Highlights the need for proper and harmonised enforcement across the EU; recommends that the Commission review the types of sanctions available to enforcement authorities in the event of proven infringement, taking into consideration the possibility of introducing appropriate behavioural sanctions aimed at avoiding further infringement;

23. 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;

24. Stresses the need for the Member States to give greater powers to national judicial and data protection authorities to sanction companies for data protection breaches or failure to apply data protection laws;

25. Invites the Commission to clarify and substantiate the existing rules regarding relevance, need, efficiency, clarity and enforceability, as well as the powers, competence and enforcement activities of the authorities, so as to ensure that there is a single, comprehensive harmonised data protection framework in the EU providing a high and equivalent level of protection regardless of the type of data processing engaged in; calls for the revised legislation to be applicable and enforced across the EU as well as internationally, so that, once covered by EU law, personal data remain covered by EU law, regardless of any transfers of those data or the location of the data controller or processor, thus facilitating cross-border business without undermining the protection of individuals' personal data;

26. Believes that all personal data transfers should be subject to traceability requirements (as regards origin and destination) and that this information should be made available to the individual concerned; stresses that if an individual wishes to modify personal data held by a controller, he or she should, as the data owner, be given the option of having this request forwarded to both the original source of the data and any other controllers the data have been shared with;

27. Asks the Commission to clarify the legal accountability of personal data controllers; stresses that it should be made clear whether the first data controller or the last known controller is accountable or whether they are jointly accountable;

28. Calls on the Commission to promote the EU's personal data protection standards in all relevant international fora and agreements; draws attention, in this connection, to its call on the Commission to present a proposal to extend the application of the Rome II Regulation on the law applicable to non-contractual obligations to include violations of data protection and privacy, and on the Council to authorise negotiations with a view to concluding an international agreement enabling individuals in the EU to gain effective redress in the event of violations of their right to data protection and privacy under EU law;

29. Emphasises that the rules on security and personal data breach notification laid down under the amended telecoms framework must be mirrored in any new general instrument in order to secure a level playing field and uniform protection for all citizens.

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	9.5.2011
Result of final vote	+: 32 –: 0 0: 4
Members present for the final vote	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Lena Ek, Ioan Enciu, Adam Gierek, Norbert Glante, Fiona Hall, Romana Jordan Cizelj, Krišjānis Kariņš, Lena Kolarska-Bobińska, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Jaroslav Paška, Herbert Reul, Amalia Sartori, Britta Thomsen, Evžen Tošenovský, Ioannis A. Tsoukalas, Niki Tzavela, Marita Ulvskog, Kathleen Van Brempt, Henri Weber
Substitute(s) present for the final vote	Matthias Groote, Françoise Grossetête, Satu Hassi, Jolanta Emilia Hibner, Yannick Jadot, Oriol Junqueras Vies, Silvana Koch-Mehrin, Vladko Todorov Panayotov, Markus Pieper, Algirdas Saudargas
Substitute(s) under Rule 187(2) present for the final vote	Alexandra Thein

14.4.2011

OPINION OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

for the Committee on Civil Liberties, Justice and Home Affairs

on a comprehensive approach on personal data protection in the European Union (2011/2025(INI))

Rapporteur: Matteo Salvini

SUGGESTIONS

The Committee on the Internal Market and Consumer Protection calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

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

B. whereas social networking sites of all types are spreading rapidly on the internet, and young people in particular divulge personal data on these,

C. whereas the core principles of the 1995/46/EC Directive remain valid, globalisation and rapid technological developments have brought new challenges in terms of personal data protection as a result of the increased reliance on complex information technology tools for data processing as well as enhanced online activity, including e-commerce, e-health, e-government, the increasing use of social networks, the development of online behavioural advertising, or cloud computing,

D. whereas the increasing exchange of individuals' personal data combined with new technological developments have led to a rise in personal data collection, storage and use, and raise the issue of determining the applicable law and defining the responsibilities of all interested parties in terms of implementation of EU data protection legislation (e.g. a firm dealing with EU citizens' personal data, whose headquarters are located outside the EU territory, and which is subcontracting to firms also located outside the EU territory),

E. whereas the revision of the Data Protection Directive 95/46/EC should comprise an

overarching reform of the EU framework for data protection law, laying out more stringent rules with regards to the collection of data, notably by informing the individual why, by whom and for how long his or her data will be collected and used, this both within the online as well as the offline environment,

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

G. whereas loyalty cards (e.g. club cards, discount cards or advantage cards) are being used more and more frequently by companies and in commerce, and are, or can be, used for customer profiling,

H. whereas the data collected via these loyalty cards are used for customer profiling; whereas a market trading in such data has been created,

1. Calls for the data protection dimension of the internal market to be enhanced through both online and offline through full harmonization of Member States' legislation, after a thorough impact assessment and by analogy to the telecom framework rules according to a very high level of protection in order to increase legal certainty, to ensure consistent levels of privacy, reduce administrative burden and costs, avoid the risk of 'forum shopping' between more or less stringent Member States' national legislation, and ensure a level playing field for all economic operators and data controllers; considers that this will boost the digital single market and reduce undue costs for businesses, especially for SMEs;

2. Believes that the implementation of EU data protection rules remains uneven and fragmented throughout the EU, consequently having an adverse effect on individuals' fundamental rights and freedoms with regards to data protection and privacy, legal security and clarity in contractual relations, the development of e-commerce and e-business, consumer trust in the system, cross border transactions and the realisation of a truly level playing field for businesses and SMEs within the Single Market;

3. Notes that data protection should play an ever greater role in the internal market;

4. Calls for a swift revision of the existing EU legislative framework on data protection, especially in view of the mounting threat to personal data posed by new forms of data processing, such as profiling or the unwanted transfer of data;

5. Calls in particular for the alignment of the data protection rules to the basic principles of the e-privacy Directive in all areas of data protection in order to avoid a fragmented approach;

6. Emphasises the demand for a functioning Single Market with regard to a coherent, comprehensive and effective enforcement of data protection rules, taking into account the impact of new technologies on individuals' rights, the transparency of procedures, and the legitimate interests of the people concerned; while ensuring portability of personal data to facilitate the smooth functioning of both the Single Market and the internet and its characteristic openness and interconnectivity;

7. Is of the opinion that any personal data and information circulated among the different Points of Single Contact and within the Internal Market Information system (IMI) are solely processed, used and collected for legitimate purposes and that necessary safeguards against abuse are put into place;

8. Highlights the importance of updating the directive in line with global technological developments;

9. Considers that profiling should, in principle, only be permitted where there is a solid legal basis, or if the persons concerned freely give their informed consent which can be revoked at any time;

10. 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 a clarification of the capacities of data controllers, data processors and hosts as to better allocate the corresponding legal responsibilities and so that the data subjects know where their data are stored, who has access to their data, who decides the use to which the personal data will be put, and what kind of back-up and recovery processes are in place;

11. Stresses the need for awareness-raising and educational activities and targeted-communication strategies on data protection for service providers, but also for citizens and consumers; Calls for the need to ensure that citizens are properly informed about their rights and obligations regarding the use of their personal data, the short and long term consequences of providing certain types of data, the different modalities of consent, the data portability, the protection of their privacy, and the tools at their disposal to prevent situations undermining their privacy as the right to be forgotten (meaning the right of individuals to have their personal data no longer collected, analysed, processed or used in any way, and deleted, when they are no longer needed for legally foreseen purposes), especially in the online sphere;

12. Calls on the Commission to reinforce, clarify and harmonise rules on free and informed consent and to clarify contract terms; demands that generally each person must give their prior consent, before their data can be collected, analysed, processed to profiles or passed on; demands also that these data must be disclosed at the request of the person concerned and also deleted at the latest when the person requests it; emphasises the need to communicate clearly to data subjects level of adequacy of data protection in third countries;

13. Emphasizes that data protection issues affect consumers and companies as well as employees; therefore calls for the inclusion of high data protection standards for employees to reduce the inappropriate monitoring of their personal data;

14. Calls on the Commission to clarify the rules related to applicable law in the field of personal data protection, as it has become increasingly difficult to determine interested parties' responsibilities given the globalisation of exchanges; underlines that it is necessary to ensure legal certainty for data controllers and avoid loopholes in the protection of personal data provided by Directive 95/46/EC;

15. Emphasises that economic activities should never be carried out without input from those

concerned; the latter must also always be given sufficient information to exercise their right to decide for themselves;

16. Draws the Commission's attention to the highly strategic nature of the location of data centres, and to the potential impact of such location outside the EU territory;

17. Welcomes the Commission's proposals for a data breach notification system in the e-privacy directive, which should furthermore be applied in a consistent manner in all areas where data protection is required; Calls for a revision and simplification of the current personal data processing notification system beyond the telecom sector to serious data breaches, with a view to ensure that data processing requirements do not place excessive burdens on data controllers and to put an end to diverging national requirements in this field; calls for an extension of the personal data breach notification system beyond the telecom sector to serious data breaches, emphasising the importance of an uniform system for notification of violations;

18. Stresses that the right of persons to decide for themselves should be brought to the fore and that each individual has the right to be informed free of charge about data collected on him/her, as well as the right to have these deleted, especially for profiles compiled for commercial purposes;

19. Emphasises the importance, for the holders of personal data, to appoint one data protection controller with a clearly identified role; considers that organisations operating in the Single Market should be able to appoint a data protection controller for their EU activities;

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

21. Underlines that the procedures on how to access personal data must be clearly and immediately available to citizens in all Member States, supported by a network of contact points, and made available online; calls in particular for the simplification of enforcement provisions;

22. Calls on the Commission to examine the modalities for access, rectification and deletion of data, as well as recourse to Alternative Dispute Resolution in the internal market; especially in the online environment; and, stresses the need for a proper infringement policy;

23. Calls for increased enforcement capacity for the national authorities, including vis-à-vis non-EU companies whose activities are targeted at EU consumers;

24. Insists on the need to promote the use of Privacy Enhancing Technologies and to implement the principle of Privacy by Design to ensure that privacy issues are included in future technological developments; Calls on the Commission to encourage technology providers to integrate core privacy principles, including data minimisation, transparency and user control, into the development and deployment of technologies in order to

guarantee a high level of protection of personal data throughout the Single Market;

25. Calls on the Commission to examine, in consultation with CEN, the possibility of developing service standards for the management of personal data and for the development of related information management tools, with due regard to the principle of privacy by design; considers that such design standards would promote best practice in the development of data management systems and improve, in particular, the security features of database management and warehousing applications; stresses however that any proposals should be technology neutral and innovation friendly;

26. Calls on the Commission to review with CEN, European hardware storage standards with due regard to the principle of privacy by design, and to encourage the development of manufacturing standards allowing for the definitive deletion of data stored on hardware which is no longer used for personal data storage or otherwise discarded; considers furthermore that such design standards would promote best practice in manufacturing; stresses however that any proposals should be technology neutral and innovation friendly;

27. Calls for an enhanced role for the Article 29 Working Party to formalise its role in implementing standard data protection rules and to assert its independence from the European Commission;

28. Calls on the Commission to carry out an impact assessment of self-regulatory initiatives as tools for better enforcement of data protection rules.

29. Encourages the development of an EU certification scheme in the field of privacy and data protection. It should be structured in a way that avoids unduly burdening companies – and particularly SMEs – with costly and bureaucratic obligations which could discourage participation. The scheme should be neutral to technology, capable of being recognised globally and affordable so as not to create barriers to entry;

30. Supports the creation of an EU certification scheme for websites that comply with EU data protection legislation, modelled on the European Privacy Seal or EuroPriSe (a voluntary trans-European label certifying the compliance of IT-based products or services with EU data protection legislation) that would be applicable throughout all the EU and replace the diversity of existing private certification schemes and labels that are often only locally recognized; considers that this should include a thorough impact assessment prior to its adoption;

31. Considers that the development and promotion of self-regulatory initiatives can improve the current framework for data protection, though they cannot take the place of legislative measures, especially in terms of enforcement; calls on the Commission and the Member States to encourage such initiative and to develop and support instruments that make it more attractive for business to agree on self-regulation;

32. Calls on the Commission not to propose too extensive a level of harmonisation that would inhibit tried and tested data protection systems such as in-house data protection controls carried out by a company's own data controllers backed up by external checks by the State data protection supervisory authorities;

33. Supports the setting-up of common and clear criteria at EU level to carry out audits in the field of privacy and data protection;

34. 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 however on the Commission to take decisive steps towards enhanced regulatory cooperation with third countries in view of clarifying the applicable rules and the convergence of EU and third country data protection legislation; calls on the Commission to bring this forwards as a priority agenda item in the re-launched Transatlantic Economic Council;

35. Calls for the development of easier, more efficient methods to allow international transfers of personal data, while assuring adequate levels of data protection and privacy of individuals;

36. Calls on the Commission to maintain the current exemptions and derogations provided by Article 9 of Directive 95/46/EC from certain data protection rules for journalistic purposes to safeguard free and independent media in the EU, and for the purpose of artistic or literary expression to support creativity;

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	13.4.2011
Result of final vote	+: 36 –: 0 0: 0
Members present for the final vote	Pablo Arias Echeverría, Adam Bielan, Lara Comi, Anna Maria Corazza Bildt, António Fernando Correia De Campos, Jürgen Creutzmann, Christian Engström, Evelyne Gebhardt, Louis Grech, Małgorzata Handzlik, Iliana Ivanova, Philippe Juvin, Sandra Kalniete, Eija-Riitta Korhola, Edvard Kožušník, Kurt Lechner, Toine Manders, Mitro Repo, Robert Rochefort, Zuzana Roithová, Heide Rühle, Matteo Salvini, Christel Schaldemose, Andreas Schwab, Eva-Britt Svensson, Róża Gräfin von Thun und Hohenstein, Kyriacos Triantaphyllides, Emilie Turunen, Bernadette Vergnaud, Barbara Weiler
Substitute(s) present for the final vote	Ashley Fox, María Irigoyen Pérez, Pier Antonio Panzeri, Konstantinos Poupakis, Sylvana Rapti, Olle Schmidt

14.4.2011

OPINION OF THE COMMITTEE ON CULTURE AND EDUCATION

for the Committee on Civil Liberties, Justice and Home Affairs

on a comprehensive approach on personal data protection in the European Union (2011/2025(INI))

Rapporteur: Seán Kelly

SUGGESTIONS

The Committee on Culture and Education calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Underlines the necessity of having a better and broader definition of personal data in online and digital technologies, in particular with regard to new forms of individual identification and tracking, especially in terms of HTTP cookies and Directive 2002/58/EC[1], to ensure legal certainty in the digital single market, so as to facilitate more effective data protection;

Transparency

2. Stresses the importance of informing users of the competent data protection authority as well as easy ways to access, to rectify and to delete their personal data;

3. Underlines that adequate mechanisms to record users' consent or revocation of consent, which must be explicit and not presumed, must be implemented;·

4. Recalls that internet users should have the right to be forgotten in the context of social networks and cloud computing; underlines in this respect that users should have the right to exercise control over which aspects of their personal data is publicly accessible;

5. Stresses that personal data communicated to the employer and concerning the user's professional situation should not be published or forwarded to third parties without the prior permission of the person concerned;

[1] OJ L 201, 31.7.2002, p. 37.

6. Stresses that privacy statements in general are very difficult to read and comprehend for all users, therefore encourages an informative system by which the data subject can understand how his personal data will be processed once consent is given;

Data protection for children and minors

7. Stresses the need for specific online data protection measures to protect children and minors; reiterates that media and ICT literacy should be an essential element of formal education in order to instruct children and minors on how to act responsibly and safely in the online environment;

8. Stresses that social networking providers must publish their security policies in clear and simple language and place this information in a prominent position so as to enable underage users to appreciate the dangers involved; stresses in particular that underage users should be given suitable guidance and efforts made to protect their anonymity if they use an on-line pseudonym; underlines that they should also be urged to enter the minimum amount of information on social networks and made fully aware of the dangers of releasing personal data such as photographs, telephone numbers or home addresses;

9. Therefore calls on the Member States to include instruction in media use as an integral part of the curriculum in schools and other educational establishments, including infant schools, and to offer teachers and educators appropriate opportunities for training and further training;

10. Calls for data controllers to be obliged to adopt age verification mechanisms, so long as this process does not threaten privacy or prevent legitimate consumers from accessing online services;

11. Calls for the establishment of specific obligations and requirements when processing data relating to minors, and in particular children, including a prohibition on the collection of sensitive data relating to children; suggests that the collection of personal information from minors should not be allowed unless it is for lawful purposes;

12. In collecting and processing data regarding school pupils or those attending other educational establishments, due care must be exercised and the data should only be shared after consent has been given, while respecting the paramount interests of the children concerned;

13. Suggests a system whereby the level of data protection offered is immediately apparent to the data subject before consent is given, possibly in the form of a grading system, which is overseen by an independent authority;

Raising awareness

14. Encourages the Commission and the Member States to organise public awareness campaigns aimed at minors, and in particular children and their carers, highlighting the risks to their privacy in the online environment, the steps they can take to protect themselves and the need to take their own responsibility; stresses that such information must be provided in a clear and comprehensible form; this requirement should apply in

particular to the formulation of texts which provide the basis for specific consent to the use of data;

15. Further recommends training and awareness campaigns targeted at data controllers and processors, informing them of their obligations and responsibilities;

16. Stresses the importance to maintain, and where appropriate, to reinforce, the derogation for journalistic purposes in Article 9 of Directive 95/46/EC[1] which is a necessary prerequisite for the exercise of journalistic activities in an increasingly complex technological media environment and for the fulfilment of the media's role in democratic societies.

[1] OJ L 281, 23.11.1995, p. 31.

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	12.4.2011
Result of final vote	+: 29 –: 0 0: 0
Members present for the final vote	Magdi Cristiano Allam, Maria Badia i Cutchet, Zoltán Bagó, Malika Benarab-Attou, Lothar Bisky, Piotr Borys, Jean-Marie Cavada, Silvia Costa, Santiago Fisas Ayxela, Mary Honeyball, Petra Kammerevert, Emma McClarkin, Marek Henryk Migalski, Katarína Neveďalová, Doris Pack, Chrysoula Paliadeli, Marie-Thérèse Sanchez-Schmid, Marietje Schaake, Marco Scurria, Joanna Senyszyn, Hannu Takkula, László Tőkés, Helga Trüpel, Gianni Vattimo, Marie-Christine Vergiat, Sabine Verheyen, Milan Zver
Substitute(s) present for the final vote	Nadja Hirsch, Seán Kelly

25.5.2011

OPINION OF THE COMMITTEE ON LEGAL AFFAIRS

for the Committee on Civil Liberties, Justice and Home Affairs

on a comprehensive approach to personal data protection in the European Union (2011/2025(INI))

Rapporteur: Françoise Castex

SUGGESTIONS

The Committee on Legal Affairs calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following suggestions in its motion for a resolution:

1. Stresses that the rapid pace of technological development in the global information society calls for comprehensive and coherent rules on data protection; notes that, following the entry into force of the Lisbon Treaty and the Charter of Fundamental Rights becoming legally biding, Article 16 of the Treaty on the Functioning of the European Union (TFEU) could provide a specific legal basis for the adoption of one legal instrument on the protection of personal data, if based on the highest level of protection provided for in EU legislation, and that this would provide greater legal certainty; whereas Article 8 of the Charter must be fully complied with in this respect;

2. Considers that this increasing complexity of data protection issues and the current lack of harmonisation between Member States' national laws call for the adoption of a comprehensive legal instrument at European level; calls, in this connection, on the Commission to establish a personal data breach notification system along the lines of that introduced by the ePrivacy Directive regarding the telecommunications sector;

3. Calls on the Commission to seize the opportunity to consolidate and reinforce a high level of protection for data subjects, so as to improve European data protection legislation;

4. Stresses that the right of access covers not only full access to data processes affecting the data subject, including the 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;

5. Calls on the Commission to guarantee synergies between data protection rights and consumer rights;

6. 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; believes that national data protection authorities should conduct awareness-raising campaigns targeting minors in particular;

7. Calls on the Commission to take account of the risk of 'forum shopping' in its proposals on determining applicable law;

8. Maintains that transparency should be established as the general principle governing the processing of personal data, as this would make it easier for individual data subjects to check their own data;

9. Strongly endorses the Commission communication when it comes to informed consent as a basic principle and asks it to clarify and strengthen the relevant rules;

10. 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;

11. Welcomes the Commission's decision to consider how a personal data breach notification requirement might be established on a general basis, bearing in mind that such a requirement at present applies to the telecommunications sector only;

12. Calls on the Commission to propose specific measures for children, who are not always aware of the risks involved in the use of the internet;

13. Points out that revision of the European rules must not entail excessive costs for European firms, as this would adversely affect their competitiveness in relation to rivals from non-EU countries;

14. Considers that self-regulation, for instance through codes of conduct, should be encouraged;

15. Points out that protection of personal data applies to everyone, but the enforcement of this right must not serve to protect criminal activities or offenders; notes that Article 47 of the European Charter of Fundamental Rights provides for the right to an effective remedy in the event of violation of rights and freedoms guaranteed by EU law;

16. Supports efforts further to advance enforceable and binding self-regulatory initiatives based on the legal framework within the revision on the data protection framework, as suggested in the Commission communication, and is in favour of further support for EU certification schemes; points out that the public procurement sector should play an important role by taking the lead here;

17. Strongly endorses the Commission communication and asks the Member States to ensure that national data protection authorities are provided with appropriate powers and own resources allowing them to properly perform their tasks at the national level and to guarantee their independence;

18. Calls on the Commission to continue the dialogue with non-EU countries with a view to establishing a coherent international legal framework, given that cloud computing and other technological developments enable controllers to operate in more than one country; calls on the Commission also to strengthen the concept of 'binding corporate rules' in the field of international data transfer;

19. Calls on the Commission to take measures in order to reaffirm and strengthen the place and role of the Article 29 Working Party in order to ensure its impartiality and the transparency of its activities, to improve cooperation between national authorities and to enhance harmonisation as regards the implementation of rules on personal data protection; At the same time, calls on the Commission to propose a legal framework making for coherence in the exercise of the powers and responsibilities of the EDPS, national data protection authorities, and the Article 29 Working Party;

20. Calls on the Commission to ensure that the directive provides clear and harmonised definitions;

21. Calls on the Commission to provide for a high level of transparency when it comes to processing of personal data in the legal framework

22. Calls on the Commission to ensure compliance with the principles of data minimisation and purpose limitation;

23. Stresses the importance of the rights of access, rectification and deletion;

24. Calls on the Commission to provide for a special restrictive regime for 'sensitive data', which will require a clear definition of this category of data;

25. Calls on the Commission to ensure that the exceptions allowed for journalistic purposes in Article 9 of the current Data Protection Directive are maintained and that every effort is made to evaluate the need to develop those exceptions further in the light of any new provisions in order to protect the freedom of the press;

26. 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.

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	24.5.2011
Result of final vote	+: 23 –: 0 0: 2
Members present for the final vote	Raffaele Baldassarre, Luigi Berlinguer, Sebastian Valentin Bodu, Françoise Castex, Christian Engström, Lidia Joanna Geringer de Oedenberg, Syed Kamall, Klaus-Heiner Lehne, Antonio Masip Hidalgo, Jiří Maštálka, Alajos Mészáros, Bernhard Rapkay, Evelyn Regner, Francesco Enrico Speroni, Dimitar Stoyanov, Alexandra Thein, Diana Wallis, Rainer Wieland, Cecilia Wikström, Zbigniew Ziobro, Tadeusz Zwiefka
Substitute(s) present for the final vote	Piotr Borys, Kurt Lechner, Eva Lichtenberger, József Szájer
Substitute(s) under Rule 187(2) present for the final vote	Pablo Arias Echeverría

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	15.6.2011
Result of final vote	+: 49 –: 1 0: 0
Members present for the final vote	Jan Philipp Albrecht, Rita Borsellino, Simon Busuttil, Carlos Coelho, Rosario Crocetta, Cornelis de Jong, Agustín Díaz de Mera García Consuegra, Cornelia Ernst, Tanja Fajon, Kinga Gál, Kinga Göncz, Nathalie Griesbeck, Sylvie Guillaume, Ágnes Hankiss, Anna Hedh, Salvatore Iacolino, Sophia in ‘t Veld, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Clemente Mastella, Véronique Mathieu, Claude Moraes, Jan Mulder, Georgios Papanikolaou, Judith Sargentini, Birgit Sippel, Csaba Sógor, Rui Tavares, Wim van de Camp, Daniël van der Stoep, Axel Voss, Renate Weber, Tatjana Ždanoka
Substitute(s) present for the final vote	Edit Bauer, Michael Cashman, Anna Maria Corazza Bildt, Luis de Grandes Pascual, Ioan Enciu, Heidi Hautala, Stavros Lambrinidis, Mariya Nedelcheva, Norica Nicolai, Zuzana Roithová, Michèle Striffler, Cecilia Wikström
Substitute(s) under Rule 187(2) present for the final vote	Marita Ulvskog, Silvia-Adriana Ţicău