Directorate-General for Justice, Freedom and Security
Unit D5 – Data protection
B - 1049 Brussels

Response to the Background Paper

This document was elaborated in response to the call for public consultation on the legal framework for the fundamental right to protection of personal data

Budapest
2010

The Association for Fair Data Processing (A Tisztességes Adatkezelésért Egyesület in Hungarian) was founded on 6th November 2009 in Budapest, Hungary. This informal association consists of independent scholars, legal and information technology experts. Its aim is to discuss newly emerging problems with respect to personal data protection and freedom of information.

In connection with the Stakeholders' Consultation "Future of Data Protection" on 1 July 2010 taken place in Brussels, the European Commission issued a background document concerning to the most relevant questions of new data protection framework. Participants were asked, if they want, send in their comments or remarks in writing up to 16th July 2010. The Association for Fair Data Processing would like to add its comments enclosed. The comments are written in *italic* while the questions are left in original style.

Budapest, 15 July 2010.

In the name of the association

Dr. Zoltán Alexin, PhD.
senior lecturer
University of Szeged,
H-6720
Árpád tér 2.
Szeged, Hungary
e-mail: alexin@inf.u-szeged.hu
web: http://www.inf.u-szeged.hu/~alexin

Member of the Scientific Advisory Committee
of the
European Privacy Institute

Dr. Pál Könyves Tóth
retired lecturer
Pázmány Péter Catholic University
H-1088
Szentkirályi u. 28-30.
Budapest, Hungary
e-mail: konyvestothpal@freemail.hu

Stakeholders' Consultations

"Future of data protection"

Background paper

1. Introduction

The Commission is currently reviewing the general EU legal instruments for the protection of personal data. With this questionnaire, the Commission seeks additional input from stakeholders on how the fundamental right to the protection of personal data can be further developed, effectively respected and enforced in the future. It also aims to structure the discussion at the targeted stakeholder consultation meetings of June and July 2010.

This questionnaire is largely based on the input collected from respondents to the 2009 public consultation, which pointed out several issues to be analysed for the purpose of improving the data protection regulatory framework and creating one consistent and comprehensive set of rules.

2. Policy objectives

The main policy objectives for the Commission are to:

- Modernise the EU legal system for the protection of personal data in all areas of the Union's activities to meet the challenges resulting from globalisation, the use of new technologies, and the needs of public authorities, in order to improve current data protection legislation as well as the effective application of data protection principles;

- Achieve consistent and effective legal implementation and application of the fundamental right to protection of personal data in all areas of the Union's activities as well as of the rules allowing their lawful free movement;

- Continue to guarantee a high level of protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States, in all areas of the Union's activities, as well as the free movement of such data;

- Ensure proper adaptation to and application of the Treaty of Lisbon's new legal bases for the protection of personal data in all areas of the Union's activities, taking into account the abolition of the former distinction between "pillars";

- Improve the clarity and coherence of the EU legal framework for personal data protection.

3. Background

Directive 95/46/EC set a milestone in the history for the protection of personal data in the EU. Many other EU policies depend on the lawful processing of personal data, not only in the area of Justice, Freedom and Security, but also in the areas of the internal market, information society, consumer protection, employment, health and competition.

Framework Decision 2008/977/JHA on the protection of personal data processed in the areas of police and judicial cooperation in criminal matters was adopted by the Council in 2008. These two instruments are complemented by other EU instruments such as Regulation (EC) n° 45/2001 regulating the processing of personal data by EU institutions and bodies and by Directive 2002/58/EC on privacy and electronic communications ("e-Privacy" Directive)[1].

With the entry into force of the Lisbon Treaty on 1 December 2009, the Charter of Fundamental Rights became legally binding. Its Article 8 recognises an autonomous right to the protection of personal data, which is equally recognised in Article 16 (1) TFEU. Article 16 (2) TFEU provides that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. This is without prejudice to the rules for the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities in matters of common foreign and security policy (CFSP), laid down in accordance with Article 39 TEU.

In 2009 the Commission organised a wide stakeholder conference on data protection and launched a public consultation about the future legal framework for the fundamental right to protection of personal data in the EU. The public consultation was concluded in December 2009.

[1] As amended by Directive 2009/136/EC.

ANNEX

QUESTIONS FOR DISCUSSION

A. Strengthening Data Subjects' Rights

1. Should the principle of "data minimisation" be explicitly introduced in the legal framework?

   Although in medical settings the "data maximization" principle is widely used instead of data minimization. Independently from this, we think that data minimization is to be introduced. Possibly with the exception: when data is necessary for the provision of care and data subject explicitly consents. Generally, we find suitable a Summary Care Record database, which contains only the relevant and minimal information about previous health events. We would also like to remark, that when the information is not stored by a health institution it does not mean that the information does not exist or is lost. The information may still exist at the patient, who store it at home, and can present when necessary.

2. Should the current provision on automated individual decisions be made more explicit, namely by clarifying that "profiling" is prohibited?

   User Generated Content (UGC) shall be considered profiling. For example, in the case of (car) insurance to compute a contract data sheet with costs upon data entered by an anonymous user – this shall not be profiling. Also, when in large internet portals like Yahoo, Gmail, Hotmail, and AOL are generating commercials for the users upon demographic data (gender, age, country).

3. Should the current categories of "sensitive data" be extended to cover (and if so why):

   - biometric and genetic data?

     *We would like to make distinction between the purposes. For forensic purposes the biometric and genetic **identification data** (that does not reveal any biomedical characteristics from the data subject) can be considered as normal personal data. In this context a fingerprint (although it may contain DNA traces that theoretically can be analysed) should also be a normal personal data – as one's name, passport number, photo etc.*

     It is advised, that the new ruling would contain the definition of health data. The advised solution is that health data shall include health administration data as well, i.e. admissions to an institute (hospital, ambulance), referral to a doctor, or appointment to an examination whenever it is personally identifiable.

- a person's family history?
- minors' data?
- data of a financial nature?

  Probably when data constitutes financial secret as well. This means that personal bank account numbers or list of transactions with dates, account numbers and amounts shall belong to special categories of personal data.

- others (*please specify*)?

  It is advised that data collected by national security services from citizens shall belong to special categories of personal data. Those data, that obtained by phone tapping, communication inspecting most probably contain information about world views, beliefs, health status, personal connections, sexual behaviour, criminal events etc. The mode of collection also reasons that these data shall belong to the special category of personal data. It probably presents greater protection for innocent people, who were followed by these services.

  Sometime the concept of a written consent shall be replaced by explicit consent so as internet health portals can legally process personal health data when obtaining ***written*** *consent is impossible or requires disproportionate efforts.*

4. Should the personal data of minors be better protected? If yes, how? In that case, should there be a harmonized age limit of 18 years in line with Article 1 of the UN Convention on the Rights of the Child?

5. Should there be specific conditions for collecting personal data if they are not directly collected from the data subject?

6. How could the "right to be forgotten" be strengthened in view of data retention and the right of deletion, particularly with reference to data protection in the on-line environment? Could the introduction of an autonomous right of the data subject to, for example, explicitly ask for withdrawal of his/her personal data from a website be an effective means of addressing this issue?

   We advise that the new European ruling shall ban the working of medical archives. In the EU several member states do not have such institutions, some requires consent to put data in, while others like Hungary still systematically collect hospital discharge records from citizens. In addition to it after some years these data are available for research and the law allows personal details be published. We think that this shall be abruptly stopped. Functioning of such institutions violates Article 9 of the Strasbourg Treaty for the protection of individual with regard to automatic processing of personal data and Article 9 of the Ovideo Treaty for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine.

This violates also the right to respect the family life as it is laid down in the Article 8 of the European Convention on Human Rights.

7. Is there a need to strengthen the control of a data subject's own personal data? Could the current data protection legislation be improved by establishing a 'property right' over individuals' personal data ("data ownership")?

8. Is there a need to address the issue of "data portability" in particular in the context of protection of personal data on the Internet, but also in the offline world? Should individuals always be able to permanently retrieve their own personal data from a certain application, and move it to another without being prevented by the data controller from doing so, either practically in terms of technical standards or contractually?

   For the reasons of portability it is advised that a new data subject access right is to be created namely, right to get a digitally signed, certified, electronic copy of personal data. Such data can be communicated by e-mails, internet services, or can be stored in a personal data storage device. This would ease to accept data coming from an other data controller. In medical settings the trust in electronic data could be much bigger when it is officially certified. Such solution provides a paperless solution for data portability.

9. Should the current requirement for "unambiguous consent" of the data subject be changed to always require "explicit consent"? If so, how could a requirement for "explicit consent" be implemented and exercised in practice, particularly in the on-line environment?

   In the case of special categories of personal data the definition for the explicit consent shall be elaborated since many times it is simply a checkbox. We advise that the fact that data processing is explicitly consented shall be documented, i.e. the date, the version of the consent text, the personal data of the data subject shall be stored and archived for the whole time of the data processing.

   The definition of the consent shall be extended with the following: "The data subject shall get information about the withdrawal of his/her consent (how, where, in what circumstances, in what conditions) before giving consent."

   In the case of implied consent it is necessary that a written version shall be at the disposal of the data subject in the course of giving preliminary privacy information, and later whenever the data subject asks for it.

10. Is there a need to improve the modalities of individuals' right of access to their own data, particularly in the online environment?

11. Should data controllers be entitled to charge for a data subject's access to one's own personal data, or should this be always free of charge? Should such provisions also apply to the exercise of the data subject's right to correct, erase and block data?

We think that electronic (paperless) copies and access shall be provided free of charge at least once per year, but in the case of archived data (stored for a given retention time for some legitimate purposes), like a ten-years-old contract in a bank, data controller may charge its legitimate costs e.g. lookup or delivery expenses. When data is asked for being provided on a special medium like X-Ray film or DVD-ROM then its costs also may be charged.

12. Should precise deadlines be introduced for the controller to:

- comply with access requests by data subjects?

  Yes, generally in the shortest time, maximally in 15 days, in the case of archived data it may lengthen to 45 days.

- comply with the obligation to rectify or delete data processed in breach of data protection?

  Yes, generally in the shortest time, maximally in 30 days.

13. Should specific safeguards be introduced for the protection of personal data of data subjects with a professional or special official secrecy obligation (e.g. legal profession, medical profession)? If yes, which ones?

Yes, penalize breach of confidentiality. In the case of intentional breach or gaining financial advantage from the breach – the penalty shall be imprisonment. In simple cases fine could be applied.

Medical professionals shall have right to deny data transfer even if it is prescribed by the law. They have traditionally right not to witness before a court, then it is evident that they should have the right not to disclose sensitive information if it is not in the life interests of someone. An inquiry from the ministry or other authority cannot be so important than the word given to their patients about secrecy.

14. Is there a need for introducing an explicit principle of transparency into the legal framework in order to ensure that data subjects receive adequate and sufficient information about the collection and processing of their personal data and to enable them to make an informed choice? In particular:

a. Should the information to the data subject contain further compulsory elements, such as the competent data protection supervisory authority and its contact details?

   The name and address of the entity who is legally responsible for the data processing, the name and address of the data protection officer (DPO) when

appointed, the local code of conduct for handling inquiries for access, copy, rectification, and deletion (when, by whom, the responsible person, official address).

b. Should the obligation to efficiently display a "privacy notice" which is conspicuous, clear and intelligible to the average user be introduced?

Yes, absolutely. Both thing, the display and the clear wording for average user is necessary. It would be nice to have a detailed privacy notice reachable from the opening webpage of the data processor.

In the case, when a DPO is appointed then he or she have to make the privacy notice publicly available and need not notify the DPA according to the 18-21 Articles of the Directive. It would be nice to have a central registry of DPOs' web pages.

c. Should a uniform EU-format be introduced to comply with this obligation?

No.

15. Is there a need to increase data subjects' general awareness of their rights?

The data protection authority shall empower data subjects with teaching materials and guidelines to increase the awareness of personal rights, computerized methods, and data transfer.

16. Should there be an explicit obligation for Data Protection Supervisory Authorities to promote awareness campaigns to inform data subjects of their rights?

Yes.

17. Is there a need to clarify the existing legal framework on the processing of personal data related to health? If so:

a. What are suitable safeguards for the protection of personal data relating to health when processed for 'public health' purposes (e.g., when collected as evidence about the health of the population, outcomes from diseases such as cancer, adverse effects from drugs)?

In the case of patient registries a unified, European ruling is advised. The right to object shall be provided as in France and Germany according the current text of the Article 14 of the Directive. Patients must be informed and provided a copy of the data to be sent.

In the case of adverse drug event, only minimally necessary pseudonymised data can be forwarded. Monograms are not suitable in the case of rare first names or

surnames. If personal identification is needed then it must be done in the presence of the data subject and his or her doctor who sent in the adverse event notice.

b. Should there be further safeguards for the protection of personal data relating to health, other than the existing requirement that processing may only take place by a health professional subject to the obligation of professional secrecy?

We do not agree that personal health data must be stored at health institutions on a data sharing network. Therefore it is advised to elaborate such a legal environment that allows patients have their health data stored on a personal storage device (Pen drive, DVD-RW, SD RAM, etc.) The solution could be such a system that ensures that all documents are certified i.e. digitally signed by a physician. In this case, patients in fact have control over their data. Retaining health data by the force of the law is allowed only to safeguard the points of Article 13 of the Directive.

Data subjects must have right to ask for deletion any personal data concerning to them when the retention time elapsed. The retention time can only be determined by the legal (criminal) responsibility of medical professionals. When this elapsed, deletion of the data must be put in the hands of the patients. See R (97) Recommendation No. 5, Article 10.

Patients shall be provided right to get anonymous medical care in simplest cases, i.e. when seeking only medical advice (like family planning advice), or regular check up without intervention.

Data subjects must have right to decide whether they are taking the services of a health insurance company (fund). It means that in those member states that owe national health system and general public health insurance, patients should have the right to pay for their health care provision a price that is publicly available, preferably is the same as the health insurance company would pay for, so as the health insurance fund not to get personal information about the care event. Everyone should have the right to get medicine full price (without subsidization) for the same reason.

The extent of personal data processing outside of health institutions has to be reduced. Laboratories, pharmacies, optometrists spas etc. can retain minimal amount of health data for a minimal time or upon specific written consent. Such data shall not be forwarded anywhere except to an insurance company (fund) when necessary.

The precondition for participating in a medical research shall be consent. If someone objects, then it must be respected, see Article 14 in the Directive.

c. Should there be a specific provision addressing the further use of personal data relating to health (e.g. by third parties for profit-making activities)?

Data subjects must know about it and they shall have right to object against to it. If we consider this usage as an infringement of personal private life, then it makes not too much difference.

18. Should there be specific rules for the processing of personal data in the employment sector? If so:
    a. What issues should be further specified?
    b. Would the explicit consent of the data subject be a sufficient and appropriate ground for lawful processing in the employment sector, given the unbalance between the worker and the employer?

    In these circumstances we can hardly speak about free consent. It is advised to rule out whether employees can consent to personal data processing related to them or cannot.

    c. Is it necessary/opportune to clarify further the conditions/safeguards for processing specific workers' data 'e.g., biometric data, drug and alcohol testing data, Internet/email and other monitoring data?

    Further dispute is needed whether the new legal framework may let member states to pass a law on surveillance of employees. The framework shall establish a good balance between privacy rights of employees and the interests of employers and also shall give protection to the collected data.

19. Is there a need to clarify the interpretation of "statistical data" and "data for scientific purposes"?

    For the clear understanding it shall be done. Statistical data must be aggregated from sufficiently many individual cases. Data for scientific purposes shall be attributed as anonymous when re-identification is practically not possible taking into account the development of the technology and those means that a third party for re-identification may reasonably use. Otherwise data can be processed upon explicit consent of data subjects.

20. Is there a need to complement the existing legal framework with specific rules on video-surveillance? If so, for which purposes?

    When no recording is taken place –surveillance in public places in general will not infringe right to private life – it has already been strengthen by the ECtHR and ECJ.

21. Does the current framework provide an appropriate balance between the protection of personal data and the need to process such data for journalistic purposes or for the purpose of artistic and literary expression, and in general the fundamental right to freedom of expression?

    Such uses of personal data may infringe the rights of the data subjects only in exceptional cases.

22. Is there a need to introduce a complaint mechanism, including on-line access requests to the data controller?

23. Is there a need to strengthen the current provisions on judicial redress? More specifically: should the possibilities for judicial redress be extended, in particular by way of "collective redress" in data protection matters?

    We would welcome the possibility of collective judicial redress. Such redress would be necessary to stop certain data processing by the decision of a court in those cases when not all data subjects are willing to enter into the trial.

24. Is there a need to develop alternative dispute resolutions (ADRs) and out-of court proceedings in data protection matters?

25. Should there be a specific provision on the protection of personal data of dead persons?

    Sometimes personal data relates not to a single person but to a whole family. This is true for the financial data, data of properties, and especially for health data. In these cases when the data subject dies, the data left behind will not loose its personal characteristics because the data still relates to other family members, especially to the children and the spouse of the data subject. Therefore the data shall be further protected.

    As the Article 8 of the ECHR says, people have right not only to respect their private life but to respect their family life as well. Protecting families is the must the member states have to do. This obligation originates from our two thousand-year-long culture, it has deep roots in religion, in the human existence.

    Therefore, whenever it may reasonably be suspected that the deceased data subject have family members whom the data may relate to, it must be treated further as personal data. From the decision of the ECtHR it is known, that in rare cases, family members may have right to access to their ancestors (health) data in their life interest. We propose to provide such right; descendants may apply to a court the get access to the data. If the court decides so, (eventually in a quickened, simpler procedure) they can get the necessary information.

    Descendants may ask for deletion of the data if no overriding interest exists. Data controllers shall delete all personal data of the deceased after the legally binding

retention time elapsed as accustomed. Rights above the personal data related to a deceased person cannot be obtained by the data controller, state, government, research group etc.

As human tissue is personal data, it is suggested to the Commission to pay special attention to the deliberate human tissue removal from deceased bodies for research purposes – as it is freely done is several countries, like in Hungary. Since such data (tissue) convey many relevant and deadly important data related to the descendants.

26. Should self-regulation in the context of strengthening the data subject's rights be encouraged?

27. In general, should the data subjects' rights be made more explicit, in order to mirror the data controller's obligations?

B. Enhancing and clarifying the data controllers' responsibility - Reducing administrative burden

28. Is there a need for further harmonisation of the data protection rules at EU level? Are there practical problems affecting the free movement of data?

According to Article 8.3 of the Directive processing of health data is allowed if the conditions set out in this paragraph are fulfilled. In the 8.4 it is said that member states may process personal health data in substantial public interest as well. That includes the possibility of making of different laws that makes the processing personal health data obligatory. In the preamble (34) such cases are listed (health insurance, social subsidization). We would welcome a common and clear list of purposes when member states may make obligatory data processing. Hungary has implemented such a legal system that makes all medical data processing for some 40 purposes obligatory, and patients are not given the right to object and to legal remedy.

The Commission shall look after that Hungary did not implemented b), e) and f) points of the Article 7 of the Directive. This means that personal data processing is not automatically possible e.g. for the performance of a contract in which data subject is a party. In that case data processing is not allowed even if the data subject consents because, according to the point b) of the Article 6 of the Directive, a legitimate purpose is also needed. If such legitimate purpose is not available then this makes a substantial obstacle before the data transfer between European companies.

29. Is there a need to further harmonise, reduce and/or simplify the notification procedures to the DPAs and to ensure an effective follow-up of notifications by the national data protection authorities? If so, should the following options be explored:

- notification limited to certain categories of processing operations such as those most likely to affect the rights and freedoms of data subjects;

- lifting the obligation to notify provided that certain conditions would be fulfilled, such as the appointment of a data protection officer (DPO), the obligation to carry out a Privacy Impact Assessment (PIA) and regular audits of data processing activities;

  The accessibility data of the DPO shall be publicly available. Data subjects may afford to the DPO or to the representative of the DPO when they have questions, claims or complaints.

  Privacy Impact Analysis shall be applied in the bigger health institutions. In these institutions regular data protection audits must also be taken place.

- the development of a uniform notification model.

30. Should the current provisions on prior checking be revised? If so, how?

31. Should a general obligation for the data controller to take appropriate measures to ensure and demonstrate the compliance with data protection law be introduced?

32. Should the obligation to conduct a PIA be introduced? Should it be mandatory for the controller? If yes, what would be the threshold for such obligation?

    It would be a genuine new instrument for protection. If a data controller processes special categories of data about more than 100-200 people, then such analysis shall be elaborated.

33. Should such obligation also apply to designers and/or manufacturers of IT systems and technologies?

34. Should there be an obligation for controllers to have a DPO? If yes, what would be the threshold for such obligation?

    If all companies that currently have notification obligation would appoint a DPO then notification is not needed any more according to the Article 18 of the Directive. In that case the DPO shall make the information about the data processing publicly available.

35. To what extent should such measures (PIA, DPO) be linked to a reduction/simplification of other administrative requirements (e.g. notifications – *see also question 29 above*)?

36. Should the principle of 'privacy by design' be introduced and if so how should it be implemented concretely?

37. How can the development and use of "Privacy Enhancing Technologies" be improved?

38. Should the obligation for reporting personal data breach notifications – as currently provided for by the e-Privacy Directive - be extended? If yes, are there specific sectors where personal data breach notifications should not apply? Should a threshold be set, and if yes, where?

    The DPA shall maintain a registry about breaches that should be publicly available. We oppose any threshold, i.e. even the slightest breach should be reported.

39. Is there a need to strengthen the current provisions on sanctions? In particular, are EU harmonised criminal sanctions for a breach of the data protection rules necessary?

    Yes, breach of confidentiality shall be penalized. In the case of intentional breach or gaining financial advantage from the breach – the penalty shall be imprisonment. In simple cases fine could be applied. In the civil law the possibility of proportionate compensation shall be effectively provided. When disclosure or breach is justified, the court should decide on the amount of the compensation taking into account the data processor's responsibility. Those data processors who fail to give preliminary privacy information also shall be fined plus shall fulfil their duty retrospectively.

C. Data protection rules in the area of police cooperation and judicial cooperation in criminal matters

40. Is there a need for specific rules on personal data processing by law enforcement authorities within the future data protection framework?

41. If yes in question 40, to what extent could limitations to the rights of data subjects in this area be necessary, namely as regards:

    - the right to information
    - the right to access, rectify and delete one's own data

42. Should the conditions for law enforcement bodies having access to and processing personal data from non-police bodies or private entities be harmonised?

43. Should there be distinct regimes applicable to personal data belonging to different categories of data subjects (e.g. suspects from non-suspects, witnesses, victims, etc.)?

44. Should the current adequacy procedure for international data transfers be extended to these areas or should a specific mechanism be envisaged?

D. Applicable law and international data flows

45. Should the current provisions on applicable law be amended? If so, how?

46. Should EU data protection legislation apply for any processing of personal data of a data subject residing within the EU, notably when the controller is established outside the EU/EEA?

47. Is the current adequacy procedure satisfactory? If not, how could it be improved?

48. Is the current system of Binding Corporate Rules satisfactory? If not, how can it be improved? Should it be codified in the legal framework?

49. Should standard contractual clauses or similar arrangements also be developed for transfers between public authorities/administrations?

50. Should the EU Standard Contractual Clauses be made compulsory for data transfers?

51. Should there be a simplified adequacy procedure as regards those countries which have signed, ratified and enacted into national law both the Council of Europe Convention 108, and its Additional Protocol 181?

    We suggest that even member states shall be checked back let's say in every 10-15 years. The DPA of the state shall elaborate a document about how the national law implements the Articles of the Directive one by one. This study shall be made publicly available and any citizen from that country may send in a comment to it within a given period of time. Taking all documents into account the Commission may strengthen the approval of the target country.

52. Could the adequacy procedure be simplified also for third countries which have declared that they comply with and adhere to the International Standards on the Protection of Personal Data and Privacy (Madrid 2009), and have enacted corresponding national data protection legislation?

53. Should special procedures be provided to simplify the authorisation by national supervisory authorities for international transfers?

54. Should there be a single authorisation procedure of the contracts or BCR used for international transfers?

E. Strengthening the role of Data Protection Authorities (DPAs)

55. Is there a need to clarify the concept or specific aspects of "complete independence" of national data protection authorities?

56. Should there be an explicit obligation on MS to provide DPAs with sufficient means and resources?

57. Is there a need for the enforcement powers and means of national data protection authorities to be harmonized, clarified, more detailed or strengthened, including imposing sanctions, investigating data controllers, entering premises and blocking databases?

58. Should there be an explicit obligation to cooperate between DPAs? Is there a need to streamline the tasks and working methods of DPAs to achieve more harmonisation?

59. Should the current role of the Article 29 Working Party on Data Protection be changed? If so, how?

60. How could the current supervisory system in the area of judicial cooperation in criminal matters and police cooperation be improved?

* * *