COUNCIL OF THE EUROPEAN UNION

Brussels, 15 February 2011

5980/4/11 REV 4

LIMITE

JAI 68
MI 50
DATAPROTECT 5
FREMP 8
COHOM 28
DAPIX 3

NOTE

from:	Presidency
to:	COREPER/Council
No. prev.doc.:	15949/10 JAI 922 MI 431 DATAPROTECT 82 FREMP 41 COHOM 237 DAPIX 46
Subject:	Council conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union

On 4 November 2010 the Council received a Communication from the Commission to the European Parliament and the Council on "A comprehensive approach on personal data protection in the European Union".

On 10 January 2011, the Presidency tabled draft Council conclusions on this Communication. While these conclusions contain general principles related to issues of particular interest, they obviously do not prejudice the need for careful and detailed consideration of any legislative proposal to be submitted to the Council.

The Working Party on Data Protection and Information Exchange (DAPIX) had two in-depth discussions on these Council conclusions at its meetings of 17 and 31 January 2011.

At the JHA Counsellors meetings of 3 and 14 February 2011, the revised draft Council conclusions on the above communication, set out in the Annex, were further discussed.

Following the JHA Counsellors meeting of 14 February 2011, a further technical amendment was made to recital No 3 so as to align its wording more closely to that of Article 16(2) TFEU.

COREPER is invited to submit the file to the Council.

Council conclusions of … 2011
on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union

1. **Considering** that, over the past two decades, the European Union has developed a considerable body of personal data protection legislation, starting with Directive 95/46/EC of the European Parliament and 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, Regulation (EC) No 45/2001 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, Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and 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. **Considering** that the time-honoured data protection principles laid down in this body of EU legislation are still valid and must be respected in all future legislative acts but that emerging business and technological developments in the last fifteen years require a thorough evaluation thereof;

3. **Noting** that the Treaty of Lisbon has put in place a new legal basis for the adoption of personal data protection legislation with regard to the processing of personal data by Union institutions, bodies, offices, and agencies, and by Member States when carrying out activities which fall within the scope of Union law and that the Charter of Fundamental Rights has acknowledged the right to the protection of personal data as a fundamental right;

4. **Emphasising** that full compliance with the principles of necessity, proportionality and purpose limitation should be ensured when collecting, retaining or exchanging personal data, so that they are processed in a responsible and secure manner;

5. **Recognising** that the exchange of personal data, when necessary and proportionate, is a crucial element in the cooperation between Member States in the area of police cooperation and judicial cooperation in criminal matters and requires appropriate data protection measures, which may enable the protection of individuals and even facilitate data exchange;

6. **Considering** that the European Union is firmly committed to protecting the fundamental rights and freedoms of its citizens as well as protecting their security; that privacy and security are possible and that there is no need to choose between being free and being safe and that the necessary and appropriate processing of personal data is vital in keeping the public safe;

7. **Recognising** that the right to the protection of personal data as a fundamental right applies also to police cooperation and judicial cooperation in criminal matters; and considering the need to establish specific data protection rules for the sector of police cooperation and judicial cooperation in criminal matters in conformity with the Charter of Fundamental Rights, while recalling that national security is a matter for Member States;

8. **Considering** that other relevant fundamental rights enshrined in the Charter, and other objectives in the Treaties, such as the right to freedom of expression and information and other values such as the principle of transparency have to be fully taken into account while ensuring the fundamental right to the protection of personal data;

9. **Reaffirming** the importance of data subjects' awareness concerning their data: a data subject should as a general rule be in a position to be aware of the processing of the data related to him, as this is an important means of guaranteeing his ability to know how the processing may impact his life. In that context the Commission should continue to investigate arrangements which favour transparency of processing;

10. **Recognising** that as regards the internal market dimension, lack of proper harmonisation has led to a situation where the Data Protection Directive's objective of the free movement of data is not fully achieved;

11. **Emphasising** that some basic elements of the 1995 Data Protection Directive, such as grounds for processing personal data and the data subjects' rights, are implemented differently in the Member States. Better harmonisation at a high level of data protection would be beneficial for both data subjects and data controllers;

12. **Emphasising** that the impact of new technologies on the protection of personal data must be carefully examined, in particular with regard to the need to inform data subjects in simple language about the impact of new technologies on their privacy and to provide 'privacy by default' options;

13. **Recognising** that the exponential growth of the internet and the advent of cloud computing will need to be taken into account when considering any changes to data protection rules. Any resource implications for business must be proportionate to the benefits delivered by appropriate safeguards for the more transparent processing of personal data;

14. **Recognising** that the extended use of biometric and genetic data in many areas requires special attention from the legislative point of view;

15. **Recognising** that in a globalised world the protection of personal data transferred to third countries is one of the most complex issues in the course of the review of the current legal framework. In this context it must be kept in mind that personal data are often transferred to, and then processed in, third countries without the knowledge of the individuals concerned. The current legal instruments have not been fully successful in dealing with these issues related to transfers to third countries and do not always provide adequate safeguards. The new legal framework should consider issues related to transfers to third countries and ensure that an adequate level of data protection in third countries is guaranteed when personal data are transferred and processed, taking into account the specificities in police cooperation and judicial cooperation in criminal matters;

16. **Noting** that data protection authorities have a central role in ensuring a high level of protection of individuals regarding their personal data. The independence and powers of data protection authorities should enable them to play an important part in enforcing compliance. A strong and harmonised role for data protection authorities in a well-regulated legal framework is essential both for data controllers and for data subjects, who can then rely on the independence of investigations carried out by data protection authorities and are entitled to expect the same level of protection in all Member States;

17. **Emphasising** that while these conclusions contain general principles related to issues of particular interest, they do not prejudice the need for careful and detailed consideration of any legislative proposal to be submitted to the Council;

The Council of the European Union

1. **Welcomes** the Communication from the Commission to the European Parliament and the Council - " A comprehensive approach on personal data protection in the European Union " and strongly supports the aim outlined in the Communication according to which appropriate protection must be ensured for individuals in all circumstances;

2. **Highlights** the fact that data protection is by its very nature horizontal in character. Within the scope of European Union law, a new legal framework based on the comprehensive approach should guarantee that appropriate data protection standards are complied with in all areas where personal data are processed;

3. **Considers** that the revision of the data protection legal framework on the basis of Article 16 TFEU offers an opportunity to improve the rules on data protection; the inclusion of provisions on data protection in the field of police and judicial cooperation in criminal matters in the new framework, should be considered, taking due account of the specific nature of these fields and of the evaluation of the implementation of 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;

4. **Shares** the view expressed in the Commission communication that the notion of a comprehensive approach to data protection does not necessarily exclude specific rules for data protection for police and judicial cooperation in criminal matters within this comprehensive protection scheme and encourages the Commission to propose a new legal framework taking due account of the specificities of this area; certain limitations have to be set regarding the rights of individuals in the specific context in a harmonised and balanced way, when necessary and proportionate and taking into account the legitimate goals pursued by law enforcement authorities in combating crime and maintaining public security;

5. **Considers** that the impact assessment for a new proposal by the Commission for a new data protection legal framework should contain a concrete cost analysis for all the new measures proposed therein;

6. **Invites** the Commission to explore the possibility of including a provision on the 'privacy by design' principle in the new legal framework and to favour privacy-enhancing technologies (PET);

7. **Demands** that special attention be given to minors who may have access to many types of IT tools and thus share their data with other users by a number of means; it believes that raising awareness in this area is extremely important, including the question of consent;

8. **Expects** the special protection of sensitive personal data to remain a core element of the Commission proposal and invites the Commission to assess whether the categories of sensitive data should be expanded against the background of new technological developments;

9. **Invites** the Commission to assess the impact of the use of biometric data on individuals, taking into account the necessity of processing of such data for specific purposes in the field of police cooperation and judicial cooperation in criminal matters, and to consider specific provisions following that assessment; the Council invites the Commission to explore the possibilities of promoting a preliminary privacy impact assessment when biometric data are processed, thus supporting the 'privacy by design' principle;

10. **Is of the opinion** that the processing of genetic data should be carried out in accordance with the principles of necessity and proportionality and considers that special provisions on aspects of cross-border processing should be explored;

11. **Supports** the idea of introducing privacy seals (EU certification schemes) and self-regulatory initiatives; both initiatives would involve close cooperation with industrial stakeholders, such as service providers, and are promising in ensuring a higher level of protection for individuals and in raising awareness. The Commission is encouraged to examine the possible role of data protection authorities in ensuring compliance in both instances;

12. **Is aware** that globalisation and technological developments have made it extremely difficult to establish the law applicable to certain cases; it feels that the new legal framework should therefore clearly regulate the issue of applicable law within the European Union in such a way so as to allow data subjects to effectively exercise their rights and to provide legal certainty to data controllers involved in cross-border activities;

13. **Holds** the view that special attention must be given to the issue of data protection within groups of companies as well as the processing of personal data in the context of employment relationships;

14. **Shares** the Commission's view that, regarding cases with an extra-EU dimension, the fact that a data controller – established within the European Union – has the processing of personal data carried out in a third country or that data are otherwise transferred to a third country on the basis of an agreement or arrangement, should not deprive data subjects of the protection of their personal data to which they are entitled, but also recognises the economic importance of technological developments and the need for legislation to reflect the economic importance to the European Union of international data transfers. The Council therefore encourages the Commission to find legal solutions that provide adequate safeguards to ensure that data subjects can exercise their data protection rights even if their data are processed outside the European Union. The new legal framework should clearly allocate responsibility in these cases and should require data controllers providing services within the European Union to inform data subjects about the details of the processing in understandable language and in a simple form. Data subjects should be in a position to ascertain if their data might be transferred to a third country;

15. **Is aware** that the development of universal principles for the protection of individuals is of utmost importance because of the globalised nature of data processing and therefore encourages the Commission especially to seek for cooperation with third countries and the development of an approach which is compatible with international organisations such as the OECD and the Council of Europe;

16. **Welcomes** the work done on drafting the principle of accountability, which highlights basic connections between different elements of the provisions: clear rules – clear allocation of responsibility – consequences of non-compliance (sanctions) – protected position of the data subject. The concept of accountability should be explored with a view to diminishing the administrative burden on data controllers, for instance by simplifying or tailoring adequate notification requirements;

17. **Invites** the Commission to explore the possibilities of using the principle of accountability and instruments of self regulation which may be conducive to smoother functioning of the internal market in order to achieve a higher level of compliance with data protection rules;

18. **Supports** the efforts of the Commission in drawing up EU standard privacy information notices, including the minimum set of information to be provided to data subjects and is of the opinion that while prime responsibility and accountability for the protection of personal data must rest with the data controller (who benefits from the use of such data), there is also a major need to increase the data subject's awareness of the implications of sharing his personal data;

19. **Encourages** the Commission to explore the opportunity as well as the costs to business and EU competitiveness in extending data breach notification obligations to sectors other than the telecommunications sector. Data breach notification should not, however, become a routine alert for all sorts of security breaches. It should apply only if the risks stemming from the breach can impact negatively on the individual's privacy;

20. **Encourages** the Commission to define more precisely the rights of data subjects (such as access, rectification, deletion/blocking) and the conditions under which data subjects can exercise these rights (e.g. by providing for deadlines);

21. **Is of the opinion** that the right of access should, as a rule, be exercised free of charge and that any charge should be without excessive expense;

22. **Encourages** the Commission to explore the introduction of a right to be forgotten, as an innovative legal instrument, insofar as the exercise of such a right is enabled by new technologies;

23. **Supports** a more harmonised role of data protection authorities, as this would help data subjects in exercising their rights and would also promote greater certainty for data controllers. This also holds true for the field of police and judicial cooperation in criminal matters, where, however, the powers of the data protection authorities should not interfere with specific rules set out for criminal proceedings or the independence of the judiciary;

24. **Agrees** with the aim of lessening the administrative burdens of data controllers and encourages the Commission to review the current requirements of notification;

25. **Supports** the Commission's aim of enhancing the data controller's responsibility and encourages the Commission to include in its impact assessment an evaluation of the possible appointment of Data Protection Officers, while not wishing to impose any undue administrative or regulatory burdens;

26. **Recognises** that the most important element of a well-harmonised approach in Member States is a new legal framework providing for a higher level of harmonisation than the current one. Further harmonisation and readjustment of the role of data protection authorities are also needed, as they have an important role in ensuring the harmonised application of rules relating to the protection of personal data. This goes especially for cases involving cross-border elements. To achieve this, the coordination between data protection authorities needs to be improved. For this reason, the role of the Article 29 Working Party should be reviewed, with special attention to the transparency and the effectiveness of the cooperation function. The independence of national data protection authorities remains the cornerstone of this cooperation.