



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 21 January 2011

**17923/1/10
REV 1**

LIMITE

**JAI 1076
MI 549
DATAPROTECT 100
FREMP 48
COHOM 299
DAPIX 57**

NOTE

from:	Presidency
to:	Delegations

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 a first in-depth discussion on these Council conclusions at its meeting of 17 January 2011. A second meeting is scheduled for 31 January 2011.

Following the DAPIX meeting of 17 January 2011, delegations will find in Annex the Presidency's revised draft Council conclusions on the above communication. In addition to the amendments made in order to accommodate delegations' suggestions, a number of linguistic changes have been made. The following delegations entered a general scrutiny reservation on the proposal: DE, DK, EE, FI and IT.

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 thereof¹;

3. **Noting** that the Treaty of Lisbon has put in place a new legal basis for the adoption of comprehensive personal data protection legislation and that the Charter of Fundamental Rights has acknowledged the right to the protection of personal data as a fundamental right;

¹ UK suggestion.

4. **Considering** that the European Union is firmly committed to protecting the security of individuals and to protecting their fundamental rights and freedoms; and that the necessary and appropriate processing of personal data is vital in keeping the public safe; it is important to defend both fundamental rights and security in order to reduce encroachment on data subjects' freedoms while still providing effective protection from terrorism and crime²;
5. **Emphasising** that full compliance with the principles of necessity and proportionality should always be ensured when collecting, retaining or exchanging personal data, so that they are processed in a responsible and secure manner³;
6. **Recognising** that the right to the protection of personal data as a fundamental right applies to police and judicial cooperation in criminal matters; and considering the need to establish specific data protection rules for the police and the judicial sector in conformity with the Charter of Fundamental Rights⁴, while recalling that national security is a matter for Member States⁵;
7. **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 data⁶;
8. **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;

² Based on UK suggestion.

³ UK suggestion.

⁴ NL suggestion.

⁵ UK suggestion.

⁶ SE suggestion. The balance with other fundamental rights is an important part of the current legal framework (see e.g. recital 72 and article 9 of Directive 95/46/EC and recital 31 of Council Framework Decision 2008/977/JHA).

9. **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 protection⁷ would be beneficial for both data subjects and data controllers;
10. **Recognising** that the exchange of personal data is a crucial element in the cooperation between Member States in the area of police cooperation and judicial cooperation in criminal matters;
11. **Recognising** that the exchange of personal data, some of it sensitive, requires stringent data protection measures. The necessary steps must be taken to enable personal data to be exchanged between Member States when it is necessary and proportionate to do so, while ensuring appropriate protection of personal data⁸;
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 rules⁹;
14. **Recognising** that the extended use of biometric and genetic data (...) in many areas requires special attention from the legislative point of view;

⁷ DE suggestion. The overhaul of the 1995 Data Protection Directive should not lead to a weakening.

⁸ Based on UK suggestion.

⁹ UK suggestion.

15. **Reaffirming** the importance of data subjects' awareness¹⁰ concerning their data: a data subject should as a general rule¹¹ 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;
16. **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 these¹² issues related to transfers to third countries and do not always¹³ provide adequate safeguards to ensure that an adequate level of data protection¹⁴ in third countries is guaranteed when personal data are transferred and processed;
17. **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;

¹⁰ NL suggestion.

¹¹ SE suggestion.

¹² UK suggestion.

¹³ AT, NL, UK suggestion.

¹⁴ NL suggestion.

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. A new legal framework based on the comprehensive approach should guarantee that appropriate data protection standards are complied with in all areas falling within the scope of European Union law¹⁵ 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 revisit the rules on data protection; following the evaluation of the implementation of Framework Decision 2008/977/JHA of 28 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters¹⁶, the inclusion of provisions on data protection in the field of police and judicial cooperation in criminal matters in the new comprehensive framework, should be considered, taking due account of the specific nature of these fields¹⁷;

¹⁵ CZ proposal.

¹⁶ Various delegations (AT, CZ, IE, LU and NL) referred to the Framework Decision 2008/977/JHA of 28 November 2008 (DPFD), the (practical) implementation of which has not yet been evaluated.

¹⁷ UK suggestion.

4. **Shares** the view expressed in the Commission communication that the notion of a comprehensive data protection legal framework does not exclude (...) specific rules for data protection for police and judicial cooperation in criminal matters¹⁸ within this comprehensive framework and encourages the Commission to propose a new legal framework taking due account of the specificities of this area; certain limitations have to¹⁹ be set regarding the rights of individuals in the specific context (...) in a harmonised and balanced way, when necessary and taking into account the legitimate goals pursued by law enforcement authorities in combating crime and maintaining public security²⁰;
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, including the implications of the possible introduction of the 'privacy by design' principle;
6. **Expects** the new legal framework to be tabled by the Commission to include a provision on the 'privacy by design' principle 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 means²¹; it believes that raising awareness in this area is extremely important (...);
8. **Expects** the special protection of sensitive personal data to remain a core element of the Commission proposal (...);

¹⁸ DE suggestion.

¹⁹ FR suggestion.

²⁰ NL suggestion.

²¹ UK suggestion.

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 and judicial cooperation in criminal matters²², and to consider²³ 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 in the context of police and judicial cooperation in criminal matters should be carried out in accordance with the principle of proportionality²⁴ and considers that special provisions on this should be explored²⁵;
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;
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;

²² Based on AT suggestion.

²³ UK suggestion.

²⁴ UK suggestion.

²⁵ Based on DE suggestion.

13. **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 (...). The Council therefore encourages the Commission to find legal solutions that provide adequate safeguards to ensure that data subjects²⁶ 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. Data subjects should always be in a position to be aware that their data might be transferred to a third country²⁷;
14. **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 international organisations such as the OECD and the Council of Europe²⁸;
15. **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; it invites the Commission to explore the possibilities of using the principle of accountability and other 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. Exemption of private data controllers from notification duties, if they are willing to declare that they are holding themselves accountable, should be explored²⁹;

²⁶ As the current data protection legislation is not restricted to EU citizens, but applies to the processing of personal data irrespective of the nationality of the data subject, the reference to EU citizens was deleted.

²⁷ DK suggestion.

²⁸ FI suggestion.

²⁹ Based on NL suggestion.

16. **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;
17. **Encourages** the Commission to explore the opportunity as well as the costs to business and EU competitiveness in extending³⁰ data breach notification obligations to sectors other than the telecommunications sector, such as financial institutions³¹. 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 individuals' privacy and their personal data and if the notification helps to protect the interests of individuals;
18. **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);
19. **Is of the opinion** that the right of access can, as a rule, be exercised free of charge or without excessive expense. All charges related to the exercise of the right of access must be justified;
20. **Encourages** the Commission to explore the introduction³² of a right to be forgotten, as an innovative legal instrument, insofar as the exercise of such a right is enabled by new technologies;

³⁰ UK suggestion.

³¹ LU and FR suggested listing these sectors. The Presidency thinks this cannot be done in an exhaustive manner in the context of these Council conclusions.

³² Based on DE and FR suggestion.

21. **Supports** a more harmonised capacity and role of data protection authorities, in the field also of police and judicial cooperation in criminal matters, while ensuring that there is a right of legal remedy from a judicial authority even where acts of the judiciary are concerned³³, as this would help data subjects in exercising their rights and would also create a more predictable area for data controllers³⁴;
22. **Agrees** with the aim of lessening the administrative burdens of data controllers and encourages the Commission to evaluate *inter alia*. the possibility of limiting the notification requirements to specific kinds of operations entailing specific risks³⁵, but is opposed to a uniform centralised EU-wide registration form/system, which could result in even more cumbersome obligations for data controllers than the current ones. A better means of achieving this goal would be the simplification of data protection registers without prejudice to any exemptions provided for in the future comprehensive legal framework³⁶;
23. **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 Officers³⁷ (...), while not wishing to impose any undue administrative or regulatory burdens³⁸;

³³ AT suggestion.

³⁴ LU queried the added value of this proposal.

³⁵ FI suggestion

³⁶ Based on NL suggestion.

³⁷ See 2.2.4, p.12 of the Commission Communication. AT scrutiny reservation.

³⁸ UK suggestion. Also FI and PT indicated there could be no general, unqualified obligation to appoint a DPO within every organisation.

24. **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 readjustment³⁹ 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.

³⁹ DE suggestion.