COUNCIL OF THE EUROPEAN UNION

Brussels, 7 December 2012

16497/12 ADD 2

LIMITE

DATAPROTECT 131
JAI 817
DAPIX 144
FREMP 140
COMIX 651
CODEC 2738

Interinstitutional File: 2012/0010 (COD)

ADDENDUM TO NOTE

from:	United Kingdom delegation
to:	delegations
No. Cion prop.:	5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217 + ADD 1 + ADD 2
Subject:	Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Delegations will find in the Annex comments from the United Kingdom delegation.

UK COMMENTS ON ARTICLES 1-8
OF PROPOSED DATA PROTECTON DIRECTIVE

6 December 2012

General Comments:

We welcome the opportunity, provided by the Presidency of the Council, to make general comments and suggested textual amendments on Articles 1-8 of the proposed Data Protection Directive. At this stage, we would want to place a general scrutiny reserve on these articles as there are a number of cross-cutting provisions that interact with later Articles and we would want to consider the package as a whole before reaching a definitive view on all the issues contained within these articles.

We are of the view that the case for repealing and replacing the Data Protection Framework Decision 2008 (2008/977/JHA) has not been made convincingly. The Framework Decision 2008 is only four years old and there is no evidence to suggest that existing arrangements do not function effectively. Further, the UK considers that the minimum standards set out in that instrument are both sufficient and appropriate for delivering fundamental rights protection in the context of police and judicial co-operation in criminal matters. Recital 48 of the Framework Decision confirms that it respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights. For these reasons the UK does not see a need for this Directive at this time.

A data protection framework should be founded on general principles and not be overly burdensome on law enforcement authorities. This draft Directive is not consistent with such an approach. Certain areas of the proposals, such as the articles on document management, data protection by design and default and breach notification, are too prescriptive and would impose disproportionate burdens on law enforcement authorities, thus undermining their operational capability.

The relationship between the Directive and the Regulation needs to be clarified. In tacking crime, reducing harm and protecting the public, UK law enforcement bodies have powers both under the civil and the criminal law at their disposal. In the course of one investigation it may be that the Directive will apply to the exercise of some powers and the Regulation to the exercise of others, such as the use of powers for civil and criminal purposes. This will result in a high level of complexity for law enforcement bodies.

The Directive should apply to authorities which exercise public functions even if they are not public authorities: In the UK functions which fall within the category of police and judicial co-operation in criminal matters are not always carried out by public authorities. The Directive should be drafted so as to apply to processing by all bodies which carry out relevant functions in the context of police and judicial co-operation in criminal matters.

The Directive should <u>not</u> apply to domestic processing. The application of the Directive to the UK is reflected in recital 75. The effect of Article 6a of Protocol 21 to the Treaties is that the Directive will only apply to data being processed under an EU instrument that binds the UK. Therefore the criminal justice system agencies within the UK will not be bound by the Directive when processing personal data outside such provisions. This means that the Directive will not apply to processing between competent authorities within the UK, where there is no cross-border dimension. The Commission have agreed to consider draft text from the UK to make the effect of recital 75 as clear as possible, which will be submitted in due course. Further, even though the provisions in the Directive relating to domestic processing will not apply to the UK we are of the view that domestic processing should be excluded for all Member States as a matter of principle on the grounds that it is inconsistent with the principle of subsidiarity. The UK considers that the form of Community action should be as simple as possible, and leave as much scope as possible for national decision. Any instrument in this area should therefore set a minimum standard and allow member states the flexibility to adopt higher standards where that is considered appropriate.

Further, UK law enforcement authorities have made the case that there is no evidence to demonstrate that the lack of EU rules in this area has had a detrimental impact on law enforcement activity or the protection of individuals. In fact, anecdotal evidence from a recent consultation exercise indicated that introducing prescriptive requirements for domestic processing may instead have a detrimental effect on law enforcement operations, placing onerous burdens on data controllers and huge costs on public authorities – without delivering better data protection for individuals. The UK therefore does not consider that full harmonisation of police and judicial co-operation in criminal matters is necessary or desirable.

ARTICLE	COMMENTARY AND PROPOSED AMENDMENTS
1. Subject Matter and Objectives	Data processing routinely engages a range of fundamental rights and freedoms, other than the protection of personal data. By way of example, the disclosure or retention of personal data can impact the fairness of a trial.
2. Scope	The UK considers that <u>domestic</u> processing of personal data should not be included within the Directive. • Suggest amendment to state: This Directive shall apply to data which are or have been transmitted or made available between Member States. • Suggest deleting recital 7 of the draft Directive on the basis that the case has not been made for the need for equivalent standards of data protection in all Member States and that this is not consistent with the principle of subsidiarity. We consider that the common minimum standards referred to in recital 3 of the framework decision are sufficient and appropriate. • Article 2(3)(a): The UK agrees that any Directive should, as now, exclude national security from its scope since this is the sole responsibility of each Member State. There should be no attempt to define 'national security' as this should be a matter for Member States. • The UK considers that minimum standards are appropriate for this instrument, in common with instruments in the area of freedom, security and justice (Title V TFEU). The UK considers that the following wording should be inserted in Article 2: "This Directive shall not preclude Member States from providing, for the protection of personal data collected or processed at the national level, higher safeguards than those established in this instrument.

	• The UK is considering the implications of the fact that scope of the Directive is different from that of the Framework Decision, in that it does not apply to processing by the Union institutions, bodies, offices and agencies. We intend to respond further on this following proper consideration. • The Framework Decision makes reference to its application to personal data which "are or have been transmitted or made available by Member States to authorities or information systems established on the basis of Title VI of the Treaty on the European Union. The UK would like to seek clarification as to why an equivalent reference is not contained with the provisions of the proposed Directive.
3. Definitions	As a general comment definitions as set out in Article 3, where appropriate, should be consistent with Article 4 - Definitions in the proposed Regulation. (1) Data Subject: • Suggest **deleting** at 3(1) and 3(2) and replacing with a single definition as in the 1995 Directive. • Support the inclusion of **"by means reasonably likely"** threshold to be used by an individual to identify an individual as this rightly excludes identification of persons by sophisticated means. • Recital 16 refers to **"means likely reasonably"** to be used whereas Art 3(1) refers to by **"means reasonably likely"** to be used – suggest recital 16 is amended to make it consistent with the language at Article 3(1). • Suggest adding an additional recital to list how an individual may be identifiable (rather than list in Article 3(1) Suggested text for recital: An individual may be identifiable, for example, by reference to any one or more of the following an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

	(2) Personal Data: • We consider that personal data should mean "any information relating to a data subject that can be used to identify that individual". As currently drafted, the text could cover information that cannot identify an individual, but relates to them. As such we consider this is linked to 3(1). • Linked to the first bullet we suggest that the definition of 'personal data' at 3(2) could be redrafted in conjunction with Article 3(1) to introduce a single definition. (6) Controller • Suggest deletion of any reference to "conditions" in Article3(6) as it is unclear the extent to which the controller would need to determine the "conditions" of processing. It is normally for the processor to determine most if not all of the conditions of processing. The controller would usually request the processor to achieve a particular outcome, leaving it for the processor to determine how this is to be achieved, especially for the larger and more established processors. This would have the unintended consequence of reducing the pool of persons that are "controllers", if all those not determining conditions are taken out of scope. • It is not considered practical to determine a threshold of conditions that need to be determined before a person is a "controller" as individuals processing situations can vary greatly. It is therefore preferable to revert to the formulation under the existing Directive. (9) Personal data breach The definition of 'personal data breach' is the same as in the current e-privacy Directive and we would want to ensure this remains for consistency with this instrument.

	(13) Child: • Suggest deletion of Article 3(13) as single definition could be problematic given the different ages of majority in Member States and the different cultural approaches to the concepts of maturity and competence. (14) Competent Authorities • As set out above, the UK considers that the Directive should apply to authorities which exercise public functions even if they are not public authorities. One solution to this issue could be to change the definition of competent authority. Another possibility might be make provision for such authorities to process data in the body of the instrument. The UK wishes to consider which alternative is most effective as the substance of the instrument is discussed in the course of working groups.
4. Principles relating to personal data processing	We consider that this should be a minimum standards instrument and would therefore argue that we should retain the wording in the existing DPFD at Article 3. • In line with the wording in the DPFD, we would recommend this article reads: 1. Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected.

	2. Further processing for another purpose shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data were collected; (b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous
5. Distinction between different categories of data subjects	**We <u>recommend</u> that this article is <u>deleted</u>** • It is neither desirable nor practical to make the distinctions that this article attempts to make. For instance, in an operational environment an individual could fall into more than one category (such as being both convicted of an offence, suspected of a related offence and a witness in another case). Given this, we are concerned that at how this will impact on working practices and system requirements. This will potentially create an additional, unnecessary and costly layer of bureaucracy, requiring re-engineering of existing systems to distinguish between categories of data subjects. • In any case, Article 4(c) already says that personal data must be adequate, relevant and not excessive for the purposes of processing. Article 5 therefore adds an unnecessary distinction which interferes with national arrangements.

6. Different degrees of accuracy and reliability of personal data	As a general comment, it is often a subjective judgement as to what is fact and what is not - we would argue that the establishment of facts is best left to the criminal courts, rather than data protection officers. **We <u>recommend</u> this article is <u>deleted</u>** • This article does not take account of operational intelligence as a category of data. In an operational environment it is not always possible to distinguish between a "fact" and a "personal assessment". This suggestion therefore has the potential to interfere with operational systems of grading intelligence, and goes beyond what is necessary for minimum standards for data protection. • In line with the above comment we recommend deletion of Recital 24.
7. Lawfulness of processing	**We <u>recommend</u> this article is <u>deleted</u>** • We consider that the minimum standards set out in the DPFD are both sufficient and appropriate for delivering fundamental rights protection in the context of police and judicial co-operation in criminal matters. Therefore, we consider that the conditions that personal data is processed lawfully, fairly, and accurately as set out in Article 3 of the DPFD should be retained (in line with comments above for Article 4 – principles relating to personal data processing).
8. Processing of special categories of personal data	We consider that there is insufficient derogation of when such data needs to be processed for legitimate criminal justice matters. And, in line with our previous argument in this response on minimum standards we would argue for reverting to the formulation of wording in Article 6 of the DPFD which states that processing is allowed "only when it is strictly necessary and when the national law provides adequate safeguards". There is also a question over whether the circumstances of processing are at least equally as important as the categories of processing and we would want to give further consideration to this matter.