



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 9 December 2013

**Interinstitutional File:
2012/0010 (COD)**

**14901/13
ADD 4**

LIMITE

**DATAPROTECT 146
JAI 903
DAPIX 129
FREMP 153
COMIX 564
CODEC 2287**

ADDENDUM TO NOTE

from: United Kingdom delegation
to: Working Party on Information Exchange and Data Protection

No. prev. doc.: 11624/1/13 DATAPROTECT 83 JAI 570 DAPIX 90 FREMP 96 COMIX 403
CODEC 1618

No. Cion prop.: 5833/12 DATAPROTECT 6 JAI 41 DAPIX 9 FREMP 8 COMIX 59 CODEC 217

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
- Chapters I-IV

Delegations will find below comments from the United Kingdom delegation on the above proposal.

General Comments

We welcome the opportunity, provided by the Presidency of the Council, to make general comments and suggested textual amendments on Chapters I to IV of the proposed Directive. We would like to reiterate our previous scrutiny reservation on the whole text.

We share the position of Denmark, Germany, and other member states that this Directive comes too soon after the Framework Decision. The latter was only adopted in 2008 and has been neither fully evaluated, nor even transposed in all Member States. Therefore we believe it is more sensible to study the benefits and shortcomings in the DPFD before trying to fix problems which may not exist.

We agree with Spain that the wording of the Directive needs to reflect the value of public interest or safety to the same extent that it reflects the value of privacy and data protection.

CHAPTER I – GENERAL PROVISIONS

Article 1 – Subject Matter and Objectives

We agree with the Member States who believe that competent authorities should not be defined as public. In the UK, as in other Member States, there has been increasing privatisation in the criminal justice sector. For example, we have recently privatised the forensic science service. Private contractors take finger prints. We feel that the text does not reflect the move towards privatisation of law enforcement activity. Spain's suggestion - that we should consider not who is in charge but the function they are performing - would be preferable.

We wish to place a scrutiny reservation on the Presidency's square brackets addition of "*maintenance of public order*" to the list of purposes. We are also considering the new suggested alternative wording from Belgium ("*the prevention of danger or risk*").

We share the concerns of other Member States about the lack of clarity in the relationship between the Directive and the Regulation, and the problems this may cause for organizations who may be caught by both instruments, depending on the exact nature of the processing they are undertaking in a given situation. We agree this risks creating a complex patchwork of rules which the police and law enforcement officials will have to attempt to disentangle.

Article 2 – Scope

We support Sweden and Denmark in that the proposed extension to internal processing does not conform with the principle of subsidiarity. Any new instrument should be restricted to cross-border transfers.

We agree with other member states that it would be helpful to provide a reference to national security in 2.3.a and would prefer the original Commission text.

Article 3 – Definitions

General Comments

Concerning a definition for consent, we would prefer to use the definition from the DPF 2008. However, we could support Slovenia's compromise suggestion of including wording in the recitals clarifying consent's relation to **Article 7**.

We would like to remove our objection in Footnote 33.

A3.10 - Genetic Data

We support the Presidency's new definition which stipulates that the data must come from an analysis of a biological sample from the individual in order to be considered genetic data. This would allay our original concerns that variables such as height and hair colour would be caught by the definition. We are still considering Austria's new suggestion to change the wording from "resulting from a sample" to "liable to be analyzed".

A3.13 – Child

We strongly support the Irish Presidency’s removal of this definition.

A3.14 – Definition of Competent Authorities

As per our concerns in Article 1, we believe competent authorities should cover situations where criminal justice activities have been contracted out to the private sector, e.g. the planned probation service reforms in the United Kingdom.

We note that in this respect the DPFD was more flexible, because the definition of a competent authority was not restricted to public authorities. Instead, the term “Competent authority” could cover a body authorised by national law to process data within the scope of the Framework Decision (see Article 2(h)).

A lack of flexibility on this point would create potential barriers to data sharing, because those Member States with significant number of private actors carrying out state functions in this area would potentially have to process a considerable amount of their criminal justice data under the Regulation.

Conversely, those who relied solely or mostly on state actors to carry out public functions in area of criminal justice processing would fall largely under the Directive. This could create confusion and undermine the purpose of the Directive which is to facilitate cross border data sharing.

Furthermore, the criminal justice system in some member states might have to operate under a data protection regime which was not designed for these purposes. The potential need for a bespoke regime for criminal justice processing is acknowledged in Recital 10 of the Directive and in Declaration 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation (annexed to the final act of the intergovernmental conference which adopted the Lisbon Treaty).

CHAPTER II - PRINCIPLES

Article 4 – Principles related to Data Processing

A4.1.3

We are concerned about the provision 4.1.3 which requires that identifiable data is kept for no longer than is necessary for the original purposes of processing. However, information may be used for multiple investigative purposes and later be required again. For example, an unsolved case may be reviewed in the future due to technological developments or additional evidence.

For this reason, we support Belgium in **Footnote 55** that states further processing for another purpose shall be permitted if it is not incompatible with the original purposes, if there are applicable legal provisions authorising the authorities and if it is proportionate and necessary.

Article 5 – Distinction between different categories of Data Subjects

We support the removal of this article from the text.

Article 6 – Different degrees of accuracy and reliability of personal data

We support the removal of this article from the text.

Article 7 – Lawfulness of Processing

General

As mentioned concerning **A4**, we would welcome a clarification about consent's relation to this provision.

A7.1.d

We agree with Germany and other member states that the words "*immediate and serious*" should be removed. A threat to public security does not need to be immediate to be of importance, for example a plot to trigger a bomb in several months. Furthermore, by their nature, all threats to public security are serious.

A7.2

We query why historical, statistical, and scientific data would be treated differently in the context of law enforcement. If the purpose is to provide evidence in a criminal case, then there is no obvious need to single out this category of evidence. If the purpose is not related to law enforcement, it would surely be caught by the proposed Regulation. It is particularly unclear as to why historical data would fall under the scope of the Directive and not the Regulation, and we feel this Article only adds to the confusion that already exists about the scope of the two instruments.

Article 7A – Specific Processing Conditions

We have no comments to make on this new article.

Article 8 – Processing of Special Categories of Personal Data

General Comments

We agree with Germany and Sweden that there should not be a general prohibition to process sensitive data. In general, we prefer the drafting in Article 6 of the DPFD.

A8.2.c

We support the Presidency's addition of an exemption in the case of preventing a threat to public security, but in line with our comments on A7, we would argue for the removal of the "immediate and serious" qualification.

Article 9 – Measures based on profiling

9.1

We would prefer the phrase "national law" in place of "a law".

9.2

We support the Presidency's provision to allow profiling which uses special category data and falls under one of the A8.2 exemptions.

CHAPTER III - RIGHTS OF THE DATA SUBJECT

Article 10 - Communication and modalities for exercising the rights of the data subject

General

We have concerns that the removal of a fee for Requests for Access could be burdensome on law enforcement bodies. Abolishing the small fee which is currently charged, and which does not cover costs, would lead to an increase in speculative requests and greater workloads.

10.5

We suggest adding the following wording from the Regulation: “*On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject.*”

We feel this addition is necessary firstly to prevent law enforcement agencies from being overburdened and secondly to promote consistency between the Directive and the Regulation.

There may also be cases where a request is of such a size that it is too much of a burden. This could be due to ignorance on the part of the Data Subject about the scale of their demand, or it may have been intended deliberately to overburden the organisation through its sheer size. We believe there should be reference to the size of the request when determining whether it is manifestly unfounded or excessive. We would suggest the wording of: “*Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, or volume...*”

Article 11 - Information to the Data Subject

A11.1

We support the Irish Presidency's restriction of the list of details required to be communicated to the Data Subject, as we believe it is too lengthy and prescriptive. However, we are still of the opinion, as expressed previously in Footnote 84, that the obligation to inform the Data Subject is too broad and burdensome for the police.

It appears that this article could be applied to the moment a suspect is arrested by a law enforcement official. It does not appear realistic to us to expect a police officer, upon arresting a suspect, to inform them of their right to complain to a Supervisory Authority about the processing of their data and the identity of the Data Protection Officer.

Article 11a - Information to be provided where the data have not been obtained from the data subject

We have no comment to make on this article.

Article 11b - Limitations to the rights of information

We have no comment to make on this article.

Article 12 - Right of access for the data subject

General Comments

We would like to see clarifications as to whether judges' notes would be covered by the right of access.

12.1

As per our suggestion for **A10**, we would recommend a provision which allows controllers to charge for copies of data along the lines of that in the Regulation:

“On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject.”

We also support the presidency's removal of 12.1.b and 12.1.h.

Article 13 – Limitations of Access

13.3

We strongly support the new provision **A13.3** from the Irish Presidency. This removes the obligation of the controller having to inform the Data Subject of their refusal, if doing so would undermine efforts to protect public security, or efforts to avoid prejudicing criminal investigations. We feel this would provide a **“Neither Confirm Nor Deny”** ability which is vital for law enforcement agencies when leading an investigation into potential suspects. We would resolutely resist any attempts to remove this article.

Article 14 - Additional modalities for exercising the right of access

We would like to place a scrutiny reservation on this Article. We have concerns that it may lead to a Controller being obliged to send the DPA very sensitive data which could prejudice investigations. A clause similar to A13.3 may be the appropriate solution.

Article 15 – Right to Rectification (including Right to Erasure formerly A16)

15.1

We have concerns over who defines “incomplete” or “inaccurate” data and how. We seek clarification about the type of data that can be rectified, for example whether this would apply to witness testimonies and personal assessments.

15.1.a

We would strongly push for a derogation to retain personal data when the controller is subject to a legal obligation. In certain instances, Police forces in the UK retain data for up to six years. The UK does not have a date from which convictions are final and no longer appealable.

We support the Presidency's change of the requirement to erase without delay to "*without undue delay*".

15.2

We believe the Controller's ability to refuse the request is not sufficiently set out here. We would prefer text similar to A13.1 and a clear stipulation that the Controller may refuse if complying would prejudice the prevention, detection, investigation, or prosecution of crime or in negatively impact public security in other ways.

We would also strongly urge for a provision limiting the obligation to communicate this refusal, similar to **A13.3** – “This shall not apply where the provision of such information would undermine a purpose under **A1**”.

It may be vital for certain investigations that suspects do not know they are under suspicion and thus have data stored about them. A “Neither Confirm Nor Deny” provision is vital here, as it is for Article 11. A suspect who unsuccessfully attempts to use **A11** to find out if they are suspected of a crime may attempt to use **A15** as a backdoor.

Article 17 – Rights of the data subject in criminal investigations and proceedings

We would seek clarification on the meaning of judicial decisions and records, and what would be included in this category.

CHAPTER IV CONTROLLER AND PROCESSOR

SECTION 1 GENERAL OBLIGATIONS

Article 18– Responsibility of Controller

General Comments

We feel this article is superfluous in relation to the rest of the Directive.

18.1.a

We support the Presidency's revised text which emphasizes proportionality and individual processing situations.

18.2

We strongly support the Presidency's removal of references to **A23**, **26-27**, and **30**. We would oppose any initiative to reinsert them.

Article 19 - Data protection by design and by default

General Comments

The United Kingdom supports the principles of data protection by design and default, but we do not believe they need to be set out on the face of legislation. We recommend that this article would be better placed in the Recitals.

We welcome the Irish Presidency's changes which take into account the scope and purposes of the processing, as well as the costs of implementation for the controller. We would oppose any reinsertion of the phrase "*state of the art*".

Article 20 - Joint controllers

We have no comment to make on this Article.

Article 21 – Processors

General Comments

We support the Presidency's removal of the requirement for the Data Processor to be considered a Joint Controller subject to **A20** if it acts without instruction from the Controller.

21.2

We query the precise meaning of a "**legal act**" and seek clarification about whether a contract is sufficient.

Article 22 - Processing under the authority of the controller and processor

We support the removal of this Article by the Irish Presidency.

Article 23 - Records of categories of personal data processing activities

General Comments

We would seek clarification on what category or type of record is required by this Article. For instance, whether it requires records listing every single individual type of processing, such as data collected upon an arrest, data processed by a custody sergeant, etc. Or if it simply requires records to be kept by categories, such as “defendant data” and “witness data”.

A23.2

We support the removal of the highly prescriptive list requiring what was to be documented. We would oppose its reinsertion.

Article 24 - Logging

A24.1

We have some concern about both the purpose and the practical difficulty of keeping such records, particularly those of erasure. This may entail disproportionate costs and burdens. We believe there should be some reference to proportionality and the cost involved.

The Irish Presidency appears to have restricted the requirement to log erasure and other actions to only automated processing systems. We would like clarification on this point.

Article 25 - Cooperation with the supervisory authority

We support the removal of this Article by the Irish Presidency.

Article 26 - Prior consultation of the supervisory authority

General Comments

We question the appropriateness for the Supervisory Authority to have oversight on law enforcement or public security matters which it may not have competence to judge. We would like to place a scrutiny reservation on this Article.

26.1

We also believe the requirement for prior consultation with the Supervisory Authority whenever a new filing systems is created is likely to be overly burdensome on Data Controllers and Processors. While we take note of the reference to risks posed to the rights and freedoms of Data Subjects, we question why the main trigger for this obligation is a new filing system. We would argue that if the Data Controller is already taking the appropriate precautions while processing special category data (**26.1.a**), prior approval should not be needed if they begin a new filing system.

We would therefore suggest the removal of **26.1.a**. For **26.1.b**, we believe there is a need for alternative wording which clearly demonstrates that the risks to the Data Subjects are new risks caused by the new technology that forms part of the new system.

26.3

We feel there are many situations involving law enforcement and intelligence where it would not be appropriate for the Supervisory Authority to comment.

SECTION 2

DATA SECURITY

Article 27 – Security of Processing

A27.2

Although we feel the list of measures to be taken is too prescriptive and doesn't reflect the needs of different situations, we support the Presidency's emphasis that the context, scope, and purpose of processing should be also taken into account. We would oppose any removal of this text.

A27.3

We welcome the Presidency's removal of the provision for the Commission to issue an implementing act.

Article 28 - Notification of a personal data breach to the supervisory authority

General

We have concerns that there may be cases where it could prejudice ongoing, sensitive investigations if a law enforcement agency is required to communicate the breach to the DPA. Again, a clause similar to A13 could be useful for such situations.

28.1

We support the removal of the notification within 24 hours by the Presidency and the replacement with "*without undue delay.*" We would resolutely oppose reversing this.

28.5-6

We welcome also the removal of the Commission's powers to issue a delegated or implementing act.

Article 29 - Communication of a personal data breach to the data subject

General

We would strongly urge for an exemption to this in situations where communicating the breach to the Data Subject might prejudice an investigation.

29.1

We strongly support the Presidency's removal of the requirement to notify the Data Subject of breaches unless the breach is likely to severely affect their freedoms and rights. We would oppose its reinsertion.

29.2

We find that the Irish Presidency's text is less prescriptive about the information that must be informed to the Supervisory Authority in the event of a breach, and we support this.

SECTION 3

DATA PROTECTION OFFICER

Article 30 - Designation of the data protection officer

30.3

We strongly support the Irish Presidency's removal of the mandatory obligation for a Data Protection Officer to be designated. We would resolutely oppose its reinsertion.

Article 31 - Position of the Data Protection Officer

We support the removal of this article.

Article 32 - Tasks of the Data Protection Officer

General Comments

We support in principle but believe that the list of tasks is highly prescriptive and could be either moved to the Recital or removed entirely.

We support the Presidency's removal of some of the requirements on the list, namely the obligation to provide documentation of compliance, as this could be an administrative burden.
