Statewatch analysis

EU data protection in police and judicial cooperation matters: Rights of suspects and defendants under attack by law enforcement demands

* the Council is removing data protection for the individual to effect the "principle of availability" (ie: that data held by one agency must be accessible to all other agencies in the EU) and seeking to ensure that nothing stands in the way of *direct/automated access* to data by the law enforcement agencies

* the Commission proposal is being fundamentally re-drafted by a Council working party representing the interests of the law enforcement agencies

* the European Parliament is only being "consulted" and has already given its opinion, now there is nothing to stop the Council re-writing the measure and nodding it through – unless the parliament insists on being re-consulted

* No principle to be established on the right of access to data held on data subjects because "in almost all cases" it would not be supplied "because of the exceptions"

* no national data protection law may "restrict or prohibit" the exchange of personal data with agencies in other EU states

* "national security matters" (internal security agencies) to be exempt from control

* admission that the main 1995 Directive ("first pillar") does not work properly in the transfer of personal data to third countries

* no obligation to correct errors or mistakes in data passed to EU states or third countries

* data to be passed to agencies in non-EU states whether they have adequate data protection laws or not under existing bilateral agreements

* to amend EU-USA agreements to meet the data protection standards would *"adversely affect the EU's credibility"*

The context[1]

The Council of the European Union (25 governments) is examining the text of a proposal for a Framework Decision on the "protection of personal data processed in the framework of police and judicial cooperation in criminal matters" (DPFD hereafter).

The draft proposal was put forward by the European Commission on 4 October 2005 and the European Parliament adopted a report on this proposal in September 2006. Under the TEU (Treaty on European Union) the parliament is only "consulted" and the final say rests exclusively with the Council.[2]

Before examining in detail the current "state of play" it is important to place the proposed measure in a historical context.

- the 1995 Directive on data protection

Commentaries on the proposed DPFD refer to the need to respect the standards set by the 1995 Directive which covers the "first pillar" (economic and social matters now including immigration).

In the "Krakow Declaration" (April 2005) the Conference of Data Protection Authorities said to avoid a "divergence" between the first and third pillars:

"The principles of Directive 95/46 should form the common core of a comprehensive European data protection law"

The first question to ask therefore is, how has the 1995 Directive been working in practice? Most of the then-15 EU member states adopted national laws by 1998 and the new members had to adopt such a law on accession.

The only review of its implementation was published by the European Commission in 2003, five years after implementation. In the middle of the report there are some sobering findings. The Commission reported that on personal data processing it was:

"hard to obtain accurate or complete information about its compliance with the law"

But anecdotal evidence and hard information, it says, suggested three inter-related problems:

---

[1] Full-text documentation is available on: Statewatch's Observatory on data protection in the EU: http://www.statewatch.org/eu-dp.htm

[2] The European Parliament can though require the Council's agreed text to be re-submitted if it differs substantially from the Commission proposal that it considered.

- *"under-resourced enforcement.. [and] enforcement actions have a rather low priority"* because of the wide range of tasks given to data protection supervisory authorities.

- *"very patchy compliance by data controllers"* because *"the risks of getting caught seem low"*

- an *"apparently low level of knowledge about their rights among data subjects"*

The Commission's report concluded that if confirmed these findings **"are reasons for serious concern".**[3] As far as is known there has been no follow-up to this report and certainly **there have been no proposals to improve the working of the 1995 Directive.**

Of direct relevance to the proposed DPFD are the rights access of individuals to the data held on them. Articles 19 and 20 of the Commission proposal lay down an obligation to provide information to the data subject **without them having to ask for it.** These Articles closely parallel Articles 10 and 11 of the 1995 Directive 95/46/EC.

The obligation to provide information, without the individual having to make a request, is set out in Article 20 where information is gathered without the "knowledge" or "awareness" of the individual.[4] In such circumstances the person is to be provided with information at least when "disclosure to a third party is envisaged".

The crucial question therefore is, if Articles 19 and 20 of the DPFD mirror those in Articles 10 and 11 of the 1995 Directive, how does this "right of information" work under the latter? For example, are people informed when their bank sends data to a credit reference agency or to an inquiry from outside their country or outside the EU? It appears there are no statistics or research on the actual practice at national level. However, the Technical Annex to the 2003 Commission report states on Articles 10 and 11:

"While some Member States stay quite close to the Directive's requirements, others have diverted considerably from them."

A similar observation is made by the Conference of European Data Protection Authorities in January 2006:

"Information communicated to the data subject.. is different from one Member State to another, some providing a lot of information while others do not

[3] In a Footnote the report says there had been a "relatively low number of individual complaints received by the Commission" and a "low number of authorisations by national authorities for transfers to third countries" which have to be notified to the Commission under Article 26.3.

[4] Article 19 covers where data is gathered with the knowledge of the individual.

communicate any information at all" (p11)

While this question is crucial, does this "right to information" under the 1995 Directive law actually work in practice, it may be quite immaterial as the present Council draft (EU doc no: 13246/06) has **deleted Articles 19 and 20** from the DPFD and even inserted the need for a **request** before there is an obligation to provide information in Article 21.

- the "principle of availability"

In response to the "war on terrorism" the "Hague Programme" (adopted on 5 November 2004 by EU governments) included a new concept, the "principle of availability", meaning that:

"throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his [sic] duties can obtain this from another Member State, and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose.." (para 2.1)

Since then a series of reports and proposed measures have sought to implement this "principle of availability". These cover specific proposals for access to fingerprints, DNA records and vehicle licensing details for starters. It is also being proposed in the Prum Treaty and in Council working parties, that agencies on country A should be given direct and automated access to the databases of agencies in country B.[5]

The draft Commission proposal reflected the "principle of availability" in Article 1.2 which said:

"Member States shall ensure that the disclosure of personal data to the competent authorities of other Member States is neither restricted nor prohibited for reasons connected with the protection of personal data as provided for in this Framework Decision"

The Council draft has retained the same intent though expressed differently, no national data protection law on data protection may "restrict nor prohibit" the exchange of personal data (EU doc no: 13246/06, Art 1.4)

Thus protection of personal data protection is to be subsumed by the "principle of availability" - coexistence is impossible.

[5] Although initially this may be on a "hit/no hit" basis after which the personal file is handed over it does not prevent an agency going on a "fishing expedition" to see if data is held on a particular individual(s)

- Data protection in the "third pillar": from the Data Protection Working Party to the Multidisciplinary Group on Organised Crime

The issue of data protection in the "third pillar" was first raised in the Council in May 1998, as the 1995 EU Directive on Data Protection did not cover justice and home affairs issues ("third pillar").

The Action Plan of the Council and the Commission on how best to implement the provisions of Amsterdam establishing an area of freedom, security and justice (13844/98) said that data protection issues in the "third pillar" should be: *"developed with a two year period"* (IV.47(a)).

A Council Working Party on Data Protection was set up in 1998 and a draft Resolution was drawn up and revised five times - the last being on 12 April 2001 under the Swedish Presidency of the EU (EU doc no: 6316/2/01) when agreement appeared to have been reached and the Article 36 Committee was asked to address outstanding reservations.

From this point on there was silence - and the Working Party was formally abolished in a re-organisation of Council's working parties in 2002.

A big shift in the handling of data protection came on 11 February 2005 when in a little noticed decision the policy brief for all data protection – including the 1995 Directive – was transferred from the Directorate-General on the Internal Market to the Directorate-General for "Freedom, justice and security" – the DG for "law, order and security" also responsible for implementing the "principle of availability" for law enforcement agencies. There was no public debate, nor any consultation with national or European parliaments.[6]

After the Commission put forward its proposed DPFD in October 2005 the Council gave the job of dealing with the issue not to a Working Party on Data Protection – comprised of member state representatives familiar with and informed on the issue – but to the Multidisciplinary Group on Organised Crime (MDG) representing the interests of EU law enforcement agencies – a bit like "putting the wolf in charge of the sheep".

Lord Avebury (UK House of Lords Select Committee on the EU) told the European Parliament on 3 October 2006 that the MDG's:

"primary interest is to make life difficult for criminals, not to have regard to the interests of data subjects"

Peter Hustinx, the European Data Protection Supervisor, expressed similar concerns to the UK House of Lords Select Committee. He said of the membership of the Multidisciplinary Group on Organised Crime that:

[6] See: **http://www.statewatch.org/news/2005/jul/06eu-data-prot.htm**

"national delegations tend to come from law enforcement areas which, up to now, largely prefer to ignore data protection".

- the issues not dealt with

There are a number of issues that the Council's draft proposal fails to address.

First, it does not cover direct/automated access by agencies to databases in another EU state.

Second, there is no distinction is made between the exchange of "hard" data (conviction, sentence etc) and "information", better termed "intelligence" which may be based on suspicion or speculation.

Police "handling codes", as they are termed, used by Europol and other police forces set out standards for evaluating the "source" and "reliability" for intelligence for non-police sources (see EU doc no: 11502/05).[7] At the top end is intelligence based on a source "who, in the past, has proved reliable in all instances" (1.A) and whose reliability "is not in doubt" (2.1). But at the other end of the scale there are sources from whom information "has in most cases proved to be unreliable" (1.C) and other sources that "cannot be assessed" (1.D.). To which can be added under reliability "information which is not known personally to the source and which cannot be corroborated" (2.4). Taken alone or in combination, for example, 1.C or 1.D together with 2.4 might suggested the intelligence is unreliable and whose exchange should be prohibited.

Doubts as to reliability can also infect intelligence recorded directly by police themselves if it is based on stereotyping or speculation.

Third, data on "non-suspects", that is, people caught up in the web of an investigation (family, friends and work colleagues) and victims. As no distinction is made in the Council draft between serious crime and any crime however minor data/intelligence on "non-suspects" who were not charged with any offence could be exchanged between agencies. The European Data Protection Authorities say that such data/intelligence should be restricted to a "limited period" and the:

"further use of these data for other purposes should be prohibited" (p7)

Fourth, Article 7 in the Council draft provides no time limits and allows different limits to be set by member states. The European Data Protection Authorities say that:

[7] In the UK these are known as "Covert Human Information Sources" (CHIS) with over 10,000 currently recorded. CHIS can be willing informers, paid informers, or induced informers (where the agencies know something against them which could be used to arrest them).

"Limited storage is a basic principle of data protection and derives from the fundamental right of respect for private life. It should not be overridden simply because a Member State chooses to legislate otherwise"

Fifth, related to time limited storage of data/intelligence there is no provision for "spent sentences" (rehabilitation of offenders) and there are major differences between member states' legislation on this area.

- the decision-making process

The DPFD deals with the exchange of personal data of a sensitive nature. As the Conference of European Data Protection Authorities observed in January 2006, in police and criminal matters:

"the consequences of the processing of personal data may seriously and harmfully affect the data subject. Indeed these data are mainly processed by authorities having public coercive powers. Moreover, the data will be exchanged on a very large scale increasing the risk of errors" (p11) [8]

And in a further Declaration in Budapest on 24-25 April 2006 they asked:

"to Member State governments to respect and strengthen the civil liberties of the citizens living in the EU when expanding the possibilities for information exchange among Member States' law enforcement authorities.. [and] recommends that the contents of the opinion adopted by the Conference of 24 January are all taken into account… " [9]

The European Data Protection Supervisor delivered an Opinion on the proposal DPFD on 19 December 2005 with detailed recommendations for changes to the Commission proposal.[10] The Conference of European Data Protection Authorities gave opinions on 24 January and 24-25 April 2006. The European Parliament agreed a report recommending sixty changes on 18 May 2006.[11]

The Council's working party, MDG, started its discussions in November 2005 but did not get down to the detail until February 2006. At the end of September the Council "first reading" was finished and its "second reading" is starting this month.

A total of nineteen documents (to date) record the detailed deliberations of the MDG – but only one is "partially accessible" on the Council register of

[8] http://www.statewatch.org/news/2006/sep/eu-dp-dpas-opinion-6329-06.pdf

[9] http://www.statewatch.org/news/2006/sep/eu-dp-dpa-budapest-statement-april-2006.pdf

[10] http://www.statewatch.org/news/2006/sep/eu-com-dp-edps-opinion.pdf

[11] http://www.statewatch.org/news/2006/sep/ep-dp-rep-18-may-06.pdf this was not formally adopted by the plenary until 27 September 2006

documents.[12]

Indeed until the MDG completes its work and the text has been agreed upstairs - in the Article 36 Committee and COREPER – we will not know what is in the final text. The intention of the Council is then to formally adopt the DPFD by "nodding it through" a Council of Ministers meeting.

The measure could go through will no time being allowed at all for data protection authorities, national and European Parliaments or civil society to look at the measure to see the changes made to the Commission draft proposal by the Council and whether recommendations for amendments had been listened to – on the evidence of the current draft (13246/06) these have been completely ignored.

To adopt such a far-reaching measure in such a way would utterly lack legitimacy.

Detailed analysis

Before starting the "second article-by-article reading" the Presidency has produced an "Issues paper" which raised major questions on which the Group was asked to give their views (EU doc 12924/06, 19 September 2006).[13] This analysis looks at these questions and others.

At the outset it should be noted that the DPFD covers the exchange of personal data for **any criminal offence however minor**.

It also covers:

"the processing of personal data wholly or partly by automatic means"

This is a reference to discussions in the Council on a number of measures under the so-called "principle of availability" which would allow agencies from another member state (or potentially a non-EU-based agency) **direct, automated access** to databases of any agency. Such access allows for no intervention to assess the nature or grounds for the request or the data accessed.

The issues raised in the Council's draft proposal are:[14]

---

[12] See Statewatch's Observatory on data protection in the EU: http://www.statewatch.org/eu-dp.htm

[13] http://www.statewatch.org/news/2006/sep/eu-dp-council-issues-12924-06.pdf It should be noted that the "issues" raised by the EU Council Presidency are *only* those issues which are "issues" for governments (and their officials) - national and European parliaments and civil society may well find other "issues" which concern them.

[14] References are based on EU doc no: 11547/3/06: http://www.statewatch.org/news/2006/sep/eu-dp-council-props-11547-rev3-06.pdf except where superseded by changes in EU doc no: 13246/06: http://www.statewatch.org/news/2006/sep/eu-dp-council-proposal-13246-06.pdf

1.1: Data held by which authorities?

The Presidency asks:

"Is it.. necessary to define the authorities with which this cooperation takes place in more detail than is provided for in the current Article 2(j)"?

Article 2.j (in EU doc 11547/3/06) says:

""competent authorities" shall mean police, customs, judicial and other competent authorities of the Member States that are authorised by national law to detect, prevent, investigate or prosecute offences or criminal activities within the meaning of Article 29 of the TEU"

Comment: Here a dilemma is raised which run through many issues in the Council's draft proposals. It could be said that the term "other competent authorities" is too general and vague and needs to be deleted and specific agencies included (see internal security agencies and Visa Information System below). Or it could be argued that if the definition is vague and general then as many bodies as possible are covered.

If the balance of the proposal is that it is really about data protection and establishes meaningful and enforceable rights for the individual then the latter position is preferable. If, on the other hand, the proposal is so infected by the "principle of availability" that it gives few enforceable rights to the data subject and *enables* the unhindered exchange of data between law enforcement agencies within, and outside, the EU then the former is preferable.

Note: The latest Council draft (13246/06) extends the scope of the measure to cover: *"the execution of criminal penalties"* in addition to the prevention, investigation, detection or prosecution of criminal offences.

1.2 Only international or also domestic processing of data?

It is proposed that the Framework Decision cover both the exchange of data between member states and the gathering and use of data domestically. This is supported by the Council Services' Legal Opinion, the Commission, the European Data Protection Supervisor and the majority of member states.

Under draft Article 1.4. member states can, at national level, provide "safeguards" that are "higher" than those in the DPFD **but** "such provisions may not restrict or prohibit" the passing of data to other member states. As the Presidency Note says:

"Member states will be under an obligation to bring their national data protection provisions into line with the DPFD"

Comment: The same dilemma arises as above. If the general standards set by the Council's draft DPFD provide, on balance, meaningful and enforceable rights for the data subjects then this should not affect rights at the national level. If, on the other hand, it would remove rights when compared to those available under 1995 Directive if data is transferred to another EU or non-EU state then it would lead to a lowering of standards.

1.3 Exchange of data with third countries

The draft proposal currently states that for the exchange of personal data with a third state (ie: non-EU) that:

"An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be passed" (Article 15.d) [15]

In the Council draft (EU doc 11547/3/06) the issue is addressed. Here five EU governments (Czech Republic, Switzerland, Finland, Greece and Portugal) support "the requirement of an adequacy finding" - that the third country meets the standard in Art 15.d.

However, seven EU governments (Germany, Denmark, Spain, Ireland, Norway, Sweden and UK):

"were opposed to the requirement for an adequacy finding"[16]

The EU Council's argument is that as:

"existing bilateral or multilateral agreements between Member States and third countries will not be affected by the DPFD.. It would hence be for each Member State to decide, in cases where there is no pre-existing bilateral treaty with a third state, to assess whether the data protection of that State is adequate"

The Council has also deleted Article 16 in the Commission's proposal which would have created a Committee for assessing whether on not a third state or international organisation had adequate data protection provisions – where it was found it did not provide adequate protection measures were to be taken to "prevent any transfer of personal data". This would at least have ensured common standards were applied across the EU.

Comment: Instead of agreeing enforceable EU standards to the transfer of personal data to non-EU states or organisations each member states can carry on

[15] Under the Commission's proposal this would cover exchanges with third states for data received from other member states. Only five EU states support this position (Czech Republic, Switzerland, Spain, Netherlands and Poland). Belgium and Hungary say it should cover all data - exchanged and domestic (EU doc 12924/06).

[16] They argued in addition that: "it did not work adequately in the context of the [1995] Data Protection Directive" - which is an extraordinary admission that requires investigation.

as now in an unregulated way. It places bilateral agreements above establishing EU common standards.[17]

It is known that the USA is opposed to adequacy findings on data protection - because it has no law protecting the data protection rights of non-US citizens. The USA is on record - in secret High-Level meetings - as saying that Article 15 (exchange of data with third countries) would:

"jeopardise the informal excellent contacts developed over time by the US law enforcement agencies with their opposite numbers in the Member States" (EU-US JHA High level meeting in Helsinki on 18 July 2006)

When the EU-USA agreements on extradition and mutual cooperation were negotiated the reverse position was taken by the EU. All 25 EU member states had to revoke bilateral agreements with the USA - because the new agreements gave the USA greater and uniform access to data and cooperation.[18]

In effect what the Council is proposing is that with the USA, for example, data and information can be given to it under existing bilateral agreements giving no protection to EU citizens whatsoever - both for the passing of the data and its further processing.[19]

1.4 National security

The Presidency Note says that:

"There is a broad consensus that processing of personal data in connection with national security purposes should be kept outside the scope of the draft Framework Decision"

The UK proposed form of words is included in the latest draft (13246/06):

"For the avoidance of doubt, this Framework Decision does not apply to national security matters"

Comment: If the Framework Decision does not cover national internal security agencies then a further Framework Decision should be put forward to cover them (like for the Visa Information System, see below).

---

17 See, for example, the experience of the Europol-USA agreement where the exchange of data/intelligence under bilateral treaties with most EU states takes precedence over exchanges under the agreement: http://www.statewatch.org/news/2006/jul/01europol-usa.htm

18 http://www.statewatch.org/news/2003/jun/01useu.htm

19 "Information"/intelligence can includes hard facts (eg: convictions) and "soft" data (eg: suspicion and speculation).

Of course there are specific cases where it is necessary, for example, for suspected terrorist offences where data/information is needed but "national security matters" is much wider then these specific instances and therefore open to abuse and misuse.

What is quite contradictory is that at the same time as the Council is seeking to remove any controls over access by security agencies to law enforcement data/information it is discussing a Council Decision on access by the same agencies to the Visa Information System (VIS).

In the draft VIS proposal there are data protection provisions in Article 8 which refer back to this very same DPFD.[20] Moreover, **access by internal security agencies to VIS is restricted to terrorism and other serious criminal offences and data can only be exchanged between EU member states - there is no provision for passing data to third states.**

2. Further processing
Do delegations agree to apply the same principle of further processing and transmission of data in a domestic context?

The Council draft has changed that proposed by the Commission (Article 5) so that further processing is legitimate if necessary for the "prevention, investigation, detection and prosecution of criminal offences" and have added threats to "public security" and "other lawful purposes of substantial public interest".

Having proposed that transferred data - from one member state to another - can be further processed the EU Presidency is suggesting the same should apply in a domestic context too.

Comment: One of the founding principles of data protection is that data collected for one purpose should not be used for another purpose. More specifically EU law says that data should not be furthered used (processed) "for a purpose considered incompatible with the one for which they were collected" (EDPS Opinion, 12.12.05). The European Data Protection Supervisor (EDPS) put it this way in his Opinion on the original Commission proposal:

"Data, once collected by the police, might be needed to solve a completely different crime. To illustrate this, one can mention that data are collected for the prosecution of traffic offences and then used to locate and prosecute a car thief. The second purpose, however legitimate, cannot be considered as fully compatible with the purpose of the collection of data. If law enforcement authorities were not allowed to use the data for this second purpose, they could be inclined to collect data for broad or ill-defined purposes, in which case the principle of purpose limitation would loose its value as to collection."

[20] EU doc no: 11405/06. Germany has put forward even more stringent proposals in EU doc no: 12840/06.

In effect the EDPS is saying that law enforcement agencies will find a way round this rule so the principle should become "flexible".

However, given this point, the Commission's proposal should if anything have been further limited to specify what is compatible and/or covered by the further exception for law enforcement, etc. more precisely. But the Council has gone in the other direction.

The current draft of the FD (as compared to the original proposal) 'would apparently allow further processing even if that processing was incompatible with the purpose for which the data was originally collected, and for purposes well beyond crime prevention and investigation of crimes. This violates one of the founding principles of data protection, the "purpose limitation" principle, which allows data collected for one purpose to be used for other purposes only if those other purposes are compatible with the original purpose.

2.A. Processing of special categories of data

The Presidency Note does not see an issue in the re-writing of Article 6: "Processing of special categories of data". The Commission draft says:

"Article 6

Processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where

- processing is provided for by a law and absolutely necessary for the fulfilment of the legitimate task of the authority concerned for the purpose of the prevention, investigation, detection or prosecution of criminal offences or if the data subject has given his or her explicit consent to the processing, and

- Member States provide for suitable specific safeguards, for example access to the data concerned only for personnel that are responsible for the fulfilment of the legitimate task that justifies the processing."

The Council is proposing:

"Article 6

Processing of special categories of data

In addition to the conditions laid down in Article 5, Member States shall permit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life only when this is strictly necessary. Member State shall provide for suitable additional safeguards."

Comment: The Commission draft sets out a prohibition to which there are exceptions provided for by "law" and where "absolutely necessary".

The Council draft establishes no such prohibition and sets a lower standard – there is no mention of legal certainty or strict necessity.

3. Rights of the data subject

The original Commission proposal covered:

Article 19: *"Right of information in cases of collection of data from the data subject with his [sic] knowledge"*

Article 20: *"Right of information where the data have not been obtained from the data subject or have been obtained from him without his knowledge"* and

Article 21: *"Right of access, rectification, erasure or blocking*" [21]

The current position of the Council is complicated yet clear.

The majority want to get rid of Articles 19 and 20 - there are governmental reservations on Article 19 by Belgium, Czech Republic, Germany, Spain, France, Greece, Italy, Netherlands, Norway, Portugal, Sweden and UK (12 governments). There are no reservations on Article 20 because it has already been merged with Article 19.

This is because, in their view, they should deal not with "a right of the data subject" but an "obligation of the competent authorities to provide information" - this is because:

"Many delegations question the appropriateness of establishing a principle which in almost all cases would not be applied because of the exceptions"

So the Council has changed the title of Article 19 (11547/3/06) from "Right of information..." to "Obligation to provide..."

The Presidency Note ends with the following question:

"Do delegations want to retain, in some form or other, an obligation for law

[21] "Blocking" is the marking of stored personal data with the aim of limiting their processing in future"

enforcement authorities to inform data subjects that data relating to them are being processed?"

The removal of Articles 19 and 20 will remove the establishment of a general principle of the right of access for data subjects.

Article 21 as it stands in the Council draft deals with the more limited issue of "Right of access, rectification, erasure or blocking". This is not an "issue" for the Council but is one that should concern others.

In Article 21.1 the Council draft adds "upon request" into the right to obtain information on data held on a person - this is a severe limitation and would remove the obligation to inform an individual regardless of whether they had made a request. An individual would have to know, or suspect, they were under surveillance in order to make a request.

The Commission draft says the data subject can obtain:

"without constraint, at reasonable intervals and without excessive delay or expense" (Art 21.1.a, 1st indent).

The Council proposes to delete *"at reasonable intervals"*.

The Commission draft says that "confirmation" as to whether or not data relating to the subject would be provided and:

"information at least as to the purposes of the processing, the categories of data concerned, the legal basis of the processing..." (Art 21.1.a.2nd indent)

should be provided. *The Council has deleted this provision*. As a footnote in the Council draft version 11547/3/06 says:

"At the suggestion of several delegations (Denmark, Netherlands and the UK), the Presidency has deleted references to the kind of information to be provided here".

Comment: So no standards are to be set as to the information to be provided to affected individuals.

Art 21.1.a.3rd indent says in the Commission draft:

"communication to him in an intelligible form of the data undergoing processing and of any information as to their source"

The Council has deleted: "and of any information as to their source" because *"this type of operational information should not be provided in the context of data protection"* (EU doc no: 11547/3/06, footnote 102).

In the Commission draft, Art 21.3, a right of appeal against refusal or restriction of

access to the competent supervisory authority is provided for - while preserving a right to a judicial remedy. The Council draft removes the first level of appeal if national law provides for "another judicial remedy". The data subject shall only be told, on appeal, "whether the controller acted correctly or not" (Commission and Council) - the provision that a person should be told "whether any necessary corrections have been made" on appeal is deleted by the Council.

The exceptions allowed for under Art 21.2 in the Council draft are the same as those in the Commission's - however, taken in the context of the other proposed changes on the rights of data subjects by the Council they take on another meaning.

It will be recalled that above in relation to deleting Article 19 the Council says:

"Many delegations question the appropriateness of establishing a principle which in almost all cases would not be applied because of the exceptions"

As the exceptions in Article 21 are exactly the same as those in the proposed deleted Article 19 surely the same argument applies, namely, that "in almost all cases" access to data will be refused by the exceptions - which will make this provision meaningless in practice.

Article 22 in the Commission draft says that following a "request" there is an obligation to pass on rectifications, blocking and erasures to agencies to whom the data has been passed. The Council draft has added:

"unless this proves impossible or involves a disproportionate effort"[22]

This has been added at the request of Denmark, France, Greece, Netherlands and Sweden who think:

"the proposed obligation was impracticable"

So even if there are errors or mistakes in personal data passed to another EU member state or a third country there would be no obligation to correct it.

Few studies/evaluations on error rates etc are available. However, an investigation by the Danish Data Protection Agency in June 2005 found 68 errors out of a base of 443 Article 96 "alerts" on the Schengen Information System (SIS) entered by Denmark. That is, in 15% of the cases there were errors (SEE Statewatch News Online, September 2005)[[23]]

4. Speciality

[22] See Conference of European Data Protection Authorities: Brussels, 24 January 2006, p12: http://www.statewatch.org/news/2006/sep/eu-dp-dpas-opinion-6329-06.pdf

[23] See: http://www.statewatch.org/news/2005/sep/danish-dp.pdf

The Council has yet to decide whether the "speciality rule" will apply to the DPFD, namely, whether data/information requested for one purpose can be used for another. This too should surely be retained as it is a standard principle of mutual legal assistance between states.

5. Relationship to international conventions

The Presidency Note (12924/06) says that data protection provisions in international conventions, agreements and MOUs between EU member states will be: "automatically superseded by the DPFD" and that:

"Bilateral and multilateral agreements between Member States and third countries however, will not be affected by the DPFD and Member States will NOT be under an obligation to amend these" (emphasis in original)

As far as agreements concluded by the EU itself:

"the Union would normally be under an obligation to endeavour to amend these conventions, unless the DPFD explicitly states they will not be affected by the DPFD"

However, despite this "obligation" the Finnish EU Council Presidency says that whichever future Presidency handles the final proposal should: *"should indeed state so"* because:

"it could adversely affect the European Union's credibility as a negotiation partner in reneging on arrangements which have been agreed with third countries. This is all the more valid as the few Agreements which have been/will be concluded on the basis of Article 24/38 TEU are of a very recent nature"

The Council is clearly more worried about its "credibility" with the USA - with whom there are "recent" agreements on EU-USA Europol, EU-USA extradition and mutual cooperation, and EU-USA PNR (passenger name record) - than it is with its "credibility" with EU citizens.

Tony Bunyan, Statewatch editor, comments:

"This is going to be a momentous decision affecting existing national laws on data protection, and the exchange of data within the EU and around the globe. It is also going to the the foundation of the right of data protection in a host of planned and future EU measures, including the new Schengen Information System (SIS II).

The Commission draft proposal is being substantially re-written by the Council's Multidisciplinary Group on Organised Crime including removing the rights of data subjects and obstacles to the passing of data to third countries outside the EU.

Until the Council finishes its so-called "second reading" the final text will not been known - when they are intending to simply "nod" it through. If it does so without the opportunity for national and European parliaments and civil society to express their views it will utterly lack legitimacy"

Postscript

The Finnish EU Council Presidency sent a Note to the Article 36 Committee/COREPER/Council setting out some of the major issues for member states (EU doc no: 12432/06). The high-level Article 36 Committee considered the Note at their meeting on 12-13 September.

The Committee did agree that "national security should not be dealt with in the instrument". However, on two other questions no agreement could be reached ("rather evenly divided"). These were on whether the measure should cover exchanges between EU member states *and* domestic (national) processing as well and the matter of whether the exchange of data with third countries should be subject to the DPFD.

Sources

The Statewatch "Observatory" on data protection is the EU contains all the background documents – full-text - and is updated. It is on:

http://www.statewatch.org/eu-dp.htm

Tony Bunyan,
October 2006