Lord Avebury, speaking at the Joint Parliamentary Meeting on EU developments in the area of freedom, security and justice at the European Parliament on October 3, will say:

This is a rare but welcome chance to discuss the implementation of the Hague Programme's decisions on data exchange and data protection with colleagues from other European Parliaments, and maybe we should set up a closed group on the web so that Members with an interest in these matters could stay in touch with colleagues in other Parliaments.

A bit of background: the House of Lords has a Committee on the European Union, and Subcommittee F, one of seven, deals with Justice and Home Affairs. We have 70 Members working on the Committee and its Subcommittees, scrutinising a quarter of the thousand plus EU documents submitted to us each year, accompanied by an explanatory memorandum from the Government. We express views to Ministers and to the House, and we can hold any document under scrutiny, effectively preventing the government from agreeing to new EU laws until they have answered our criticisms. In addition, the Subcommittee has published reports recently on proposals for a common EU returns policy for illegal migrants; economic migration to the EU; the Hague Programme's agenda for justice and home affairs, and the EU's response to terrorism post-Madrid.

After Madrid, the European Council issued a *Declaration on combating terroriem*, which called for the simplification of exchanges of information and intelligence between law enforcement agencies of Member states, and in June 2004 the Commission proposal for enhancing access to information, including 'European information systems' by those agencies. The impetus for these developments was the need to combat terrorism, but the scope had widened by then to cover not just organised crime but crime in general[1].

By September 2004, at the JHA meeting under the Netherlands Presidency, the principle of availability had emerged in its present form. It appeared in the first draft of the Hague Programme in October, and the whole package including the principle of availability went through without debate at the Summit in November

Under these proposals, from the start of 2008 a law enforcement officer in any Member state who wants information held by a law enforcement agency in another Member state is to be given it, subject to a few conditions. The data to be covered is:

DNA profiles; fingerprints; ballistics; vehicle registration; telephone numbers and other communication data, and data in civil registers.

That, in a nutshell, is the principle of availability. At the time, Commissioner Frattini, addressing the Joint Supervisory Authorities under the Third Pillar, called for the involvement of data protection agencies from the outset. He warned, that linking the adoption of new forms of police and judicial cooperation with the adoption of data

[1] eur-lex.europa.eu/LexUriServ/site/en/com/2004/com2004_0429en01.pdf

protection guidelines was still to be hammered out, and there was no deadline for this in the Hague Programme[2].

The Commission were invited to bring forward proposals for implementing the principle of availability in which 'key conditions should be strictly observed'. These would include a guarantee of the integrity of the data; confidentiality of the data; common standards for access; respect for data protection; protection of the individual from abuse of the data, and the right of the individual to seek correction of incorrect data. The Commission produced a draft Data Protection Framework Decision[3], at the same time as the draft on the principle of availability, thus emphasising themselves the importance of the two going forward together. The DPFD would ensure that information had been processed legitimately, in accordance with privacy rights and data quality standards. It would see that exchanges between competent authorities were not prejudiced by different levels of data protection.

Unfortunately, the Ministers of the 6 largest EU countries – France, Germany, Italy, Poland, Spain and UK, the G6 – decided to go ahead with availability without data protection. At their meeting at Heiligendamm last March, they jettisoned the principle that the two decisions should proceed in parallel, and decided to implement data exchange on DNA, fingerprints and vehicle registration, irrespective of whether the DPFD had come into force or not.

The existence of informal groups of Member states is not objectionable or indeed avoidable, and there are quite a few of them, either based on regional interests such as the Nordic Cooperation Group, or particular characteristics, such as the Common Law Group. What is peculiar about the G6 Group and the Prüm Group, which gave birth to the Prüm Convention[4], is that they seek to preempt EU decision-making processes, by making arrangements of their own, and offering them to other Member states on a take-it-or-leave-it basis.

Thus the Prüm Convention, agreed by Belgium, Netherlands, Luxembourg, Germany Austria, France and Spain, which concerns transfers of the same types of data that were later considered by the G6, provides that other Member states may accede to it, and says the aim of the signatories is to incorporate the Convention into the legal framework of the EU. When the principle of availability is implemented in the domestic law of the Prüm states, therefore, it will have to be a superset of the Prüm Convention, to avoid any incompatibility with their existing obligations. The other 18 EU Member states, which had no part in the discussions on the Convention or the technical work of drafting it, will have no choice but to accept it as part of the EU justice and home affairs *acquis*.

In the case of Heiligendamm, other Member states were to be fully informed about the proposals **after** they had been decided, and were condescendingly told they could take part in their implementation. But, like members of the public in general, they were not to be given the agenda or papers for G6 meetings, let alone to be consulted

---

[2] Franco Frattini, Vice-President responsible for Justice, Freedom and Security, *Data protection in the area of Justice, Freedom and Security*, Brussels, December 21, 2004

[3] EU doc 13019, October 11, 2005, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

[4] EU doc 10900/05, July 7, 2005

about the proposals to be made. Our Committee said it would be desirable to publish agendas and working documents, though we stopped short of criticising the failure to do so. This could be explored further with the Parliaments of non-G6 Member states, if we could find a web-based mechanism for doing so.

At the very least, we said that the results of future G6 meetings should be fully publicised, rather than merely being put on the website of the Interior Ministry of the host country. This month we will see whether the UK Government have complied with that recommendation, since they are hosting the next meeting of the Group at Stratford-upon-Avon in three weeks' time. So far, the Home Office have posted no information about the meeting on their website.

The Heiligendamm meeting decided that the police should have access to Eurodac, the fingerprint database established under the first pillar to help determine which country is responsible for considering asylum applications, and to the Visa Information System, which gives states common knowledge of visas granted by each other to third country nationals. In the case of the VIS there is a separate Commission proposal for access by law enforcement agencies, with safeguards. In particular, the DPFD applies to the data, and access will not commence until the DPFD has entered into force. On Eurodac, however, there is a problem, because the legal basis on which its Regulation stands would not allow access for purposes other than vetting asylum applications. Presumably there could be a new proposal relying on Article 66 TEC as the VIS does, but the Commission has no such proposal on the table.

The European Commission says that implementation of the principle of availability will change the quality and intensity of personal data exchanges between Member states, and greatly affect the right to data protection. Direct automated access, in particular, will increase the risk of transferring illegitimate, inaccurate or out-of-date information, and the data controller will not be able to verify the legitimacy of a transmission or the accuracy of the data in each individual case. For these reasons the DPFD must be developed hand in hand with availability[5]. For the G6 to undermine the Commission, and even worse, to do it as our report says, behind closed doors, and behind the backs of the other 19 Member states, is insufferable and must be opposed.

But if the Finnish Presidency is getting on with the drafting of the DPFD, especially in the light of the comments by the European Data Protection Supervisor in his Opinion last February[6], do we need to worry?

There used to be a Council Working Party on Data Protection, but it last reported in April 2001 and was then abolished. The task of polishing up the DPFD has been given to the Multidisciplinary Group on Organised Crime (MDG), whose primary interest is to make life difficult for criminals, not to have regard to the interests of data subjects. The membership of the Group is not published, so we cannot say whether it includes anyone with expertise on data protection. But not surprisingly with a title like that, the MDG had actively watered down the DPFD by the time they finished their first

[5] Proposal for a Council Framework Decision on the Protection of personal data processed in the franmework of police and judicial co-operation in criminal matters, October 11, 2005, 13019/2005, http://register.consilium.europa.eu/pdf/en/05/st13/st13019.en05.pdf, p 6

[6] European Data Protection Supervisor. Opinion on the Proposal for a Council DPFD (COM 92005) 475 final)

reading on September 21. The Presidency tabled an Issues Paper[7] at that meeting, and in the light of the discussion they have weakened the first three chapters of the document still further in a second reading draft presented at the MDG meeting on Wednesday and Thursday this week. That document and Issues Paper were inaccessible on the Council's website last week, but they have since been posted on the site of Statewatch, whose valuable evidence greatly helped our Committee in its inquiry on Heiligendamm.

The Issues discussed are of course only those which concern EU governments, and not their civil societies. However, the European Parliament does have the power to give civil society a voice, by requiring the Commission to resubmit the Council's final text if it differs substantially from the original, as it already does[8]. That will cause a delay beyond the end of 2006, and it may be objected that the DPFD is required for SIS II, due to go live in 2007. But since there has been an unannounced slippage, and SIS II, now being scrutinised by the Lords EU Committee, will not be operational until some time in June 2008[9], there is no need for urgency. We as national Parliamentarians, as well as our MEP colleagues have a responsibility to examine the DPFD in its final shape, and particularly of looking at the answers to the ten major questions now addressed to the MDG by the Presidency[10]. In the original version, for instance, data subjects were to be told when information about them was processed or transferred, subject to exceptions on grounds of security. In the latest draft, there is no right to notification, and Member states are being asked by the Presidency whether they wish to retain some form of obligation to tell a person when data relating to her is being processed. The subject can still get certain information held, which the Presidency say should be as limited as possible, on request, but this means she has to know or suspect that she is under surveillance.

In his mid-term review of Finland's Presidency last Thursday, Prime Minister Matti Vanhanen did not mention these questions, but he did say (and I quote):

"Parliamentary accountability in EU affairs is a strong constitutional obligation - and living practice - in the Finnish political system. Parliamentary scrutiny is an inseparable part of all Finnish EU policy".

There has been no scrutiny of the whittling away by the Council and the shadowy MDG of the data protection safeguards that will apply to the millions of exchanges of personal information that will ultimately be dealt with under the principle of availability, but as Parliamentarians we still have a chance to remedy the omission.

[7] EU doc 12924/06 September 19, 2006
[8] EU doc 12924/06, September 19, 2006
[9] EU doc 13102/1/06 REV 1, September 25, 2006
[10] EU doc 12924/06, September 19, 2006