Statewatch Analysis

Lubricating the flow of information in the EU

Eric Töpfer

The EU Information Management Strategy (IMS), is meant to include a strong data protection regime. However, while the first practical steps have been taken, fundamental rights are falling behind.

The Conclusion of the Information Management Strategy (IMS) for EU Internal Security [1] was announced in the action plan for the implementation of the Hague Programme. Its conclusion was endorsed by the "Future Group", and it was eventually accepted by the Council of Justice and Home Ministers on 30 November 2009 together with the Stockholm Programme. After the presentation of a first draft by the Swedish Presidency on 16 June 2009, [2] it was mainly the Ad hoc Group on Information Exchange that negotiated the details on behalf of the Council. Although the Ad hoc group members agreed that the secret service's work should be excluded, [3] the scope of the IMS was contested. In particular, the German delegation wanted to limit its scope to the areas of law enforcement and judicial cooperation in criminal matters for reasons of effectiveness. However, the majority of delegations opted for a "holistic approach" that included customs cooperation and migration control. A compromise was found by the Committee of Permanent Representatives (COREPER), the ambassadors of the Member States to the EU, who proposed that Member States could apply the IMS by "adopting a step-by-step approach" and gradually expanding its application.

The IMS's motto is "Streamline the management of information". Given the panoply of central European databases and planned networked national information systems the aim of the strategy is to deliver a "method" to ensure "coherence and consolidation" and to ensure that existing instruments and arrangements are implemented before new initiatives are planned. The IMS in itself should:

> *"not create links between different databases or provide for specific types of data exchange, but it ensures that, when the operational requirements and legal basis exist, the most simple, easily traceable and cost-effective solution is found."*

Thus the IMS calls for inventories and analyses of needs, for the documentation of work flows and the coordination of interfaces as well as for the assessment and organisation of responsibilities for future development. The strategy values "data protection requirements".

But on the other hand it explicitly states that the daily practice of information exchange "must not be hampered by issues of competence": interoperability, the availability and seamless flow of data, should be:

"ensured whenever necessary and proportional, among and beyond the authorities directly responsible for EU internal security, but also that it is limited to these cases."

IMS in action: information mapping

For the IMS follow-up the Ad hoc Group (which in July 2010 became the permanent Working Party on Information Exchange and Data Protection (DAPIX), now responsible for technical and administrative aspects of the implementation of the "principle of availability") outlined an action list. This list, which had grown to 17 projects, [4] was narrowed down to 11 "priority actions" by March 2010 (see Table 1). [5]

Since then small project teams have been making progress on each of the actions. The first milestone in processing the action list was taken by the European Commission taking charge of priority action number one, the "information mapping project". On 20 July 2010 Home Affairs Commissioner, Cecilia Malmström, presented the Communication entitled "Overview of information management in the area of freedom, security and justice", [6] the first comprehensive update of a report on third pillar information systems that was published in 2003.

From "Advance Passenger Information" to "Visa Information System (VIS)" the overview lists 19 existing "instruments", (i.e. regulations for the implementation and operation of IT systems and cross-border information networks, for mandatory collection of data at the national level and for data transfer to third countries), (see Table 2). While some of these regulations and systems are in place and have been operating for many years, such as the Schengen Information System (SIS) or EURODAC, others have still not been fully implemented, such as the Prüm Decisions and the Data Retention Directive. In addition, the overview lists six projects which are currently under discussion: a European Passenger Name Record (PNR) System, an Entry-Exit-System for non-EU-citizens, a Registered Travellers System for fast biometric border controls for frequent flyers, an Electronic System of Travel Authorisation (ESTA) for accelerated immigration control of third-country nationals not subject to visa requirements, a European Terrorist Finance Tracking Programme (TFTP) and a European Police Record System (EPRIS).

The overview concludes by confirming the commitment to data protection, valuing in particular "privacy by design", (i.e. technical data protection solutions and the need to justify new instruments adequately). The consideration of "sunset" clauses and mandatory evaluation for future instruments is also proposed. In addition, the Conclusion seeks "to draw on the input of all relevant stakeholders", including "economic actors and civil society" when developing new initiatives and suggests that the nascent EU Agency for the Operational Management of Large-scale IT Systems, namely SIS, EURODAC and VIS, could facilitate such dialogues.

Justice Commissioner Viviane Reding's Communication for "A comprehensive approach on personal data protection in the European Union", published on 4 November 2010, points in a similar direction. [7] Noting that Council Framework Decision 2008/977/JHA on data protection in police and judicial cooperation in criminal matters only applies to cross-border exchange of data and not to data processing in the Member States themselves, and that many loopholes exist from the principle of binding purpose and that Europol's and Eurojust's computer systems and the SIS and CIS do not fall under the scope of the

Framework Decision, the Communication emphasises "the need to consider a revision of the current rules" and invites all "concerned stakeholders" for consultation.

European Data Protection Supervisor (EDPS) Peter Hustinx was pleased and expressed his support for both Malmström's and Reding's Communications. [8] He complained, however, that Malmström's overview on information management refers to alleged successes and is silent on problems and deficiencies. Indeed, the Communication surprisingly emphasises that most systems and networks for information exchange in the "area of freedom, security and justice" have a "limited purpose". Thus, it bluntly ignores the function creep inherent in most "instruments". Moreover, it suggests that proportionality is the system's rule while claiming, for instance, that the Prüm Decision's aim is to combat terrorism and serious crime, despite the fact that almost 90 per cent of Prüm "hits" occur during investigations of theft or fraud. [9] Therefore, concern is justified - even more so when given how the JHA Council's working parties, in particular the shadowy Multidisciplinary Group on Organised Crime (MDG), successfully torpedoed the Commission's weak proposal for the Framework Decision on third pillar data protection after its publication in 2005. [10]

Towards a comprehensive approach on data protection?

Indicators of the direction that the revision of the data protection framework might take in the field of justice and home affairs can be found in the reactions of the Council to the Commission's Communication and the progress of other "priority actions" implementing the IMS. After an initial brief policy debate by Justice and Home Ministers at their Council meeting on 2-3 December 2010, [11] it was the DAPIX Working Party that discussed the issue shortly before Christmas 2010. The Commission presented the Communication on data protection and, when asked whether their legislative proposals would "take into account the specific requirements of law enforcement bodies and how the impact on operational policies would be assessed", replied that the "limits of transparency for the police sector would be respected". [12]

On 10 January 2011, the Hungarian Presidency presented a first classified draft for a Council Conclusion [13] responding to the Commission's Communication which was – additionally informed by an Opinion of the European Data Protection Supervisor (EDPS) [14] – discussed twice in depth by the separate DAPIX subgroup on data protection in the course of the month. A revised draft version [15] – still secret – was discussed in the first weeks of February by JHA Counsellors, the attachés of the Permanent Representations of the Member States in Brussels. As only the fourth revision of this second draft was published in the Council's Register the detailed arguments behind closed doors remain unknown. But it is clear that far reaching revisions of the current data protection framework for police and judicial cooperation are contested by strong interests. Three days before JHA Counsellors met for the second time in Brussels to discuss the draft Conclusion, the German *Länder* adopted a Decision on the Commission's Communication arguing that the EU lacks the competence to expand the scope of the data protection regulation to domestic data processing by police and judicial authorities: "The regulations have to be limited to cross-border issues." [16]

The Conclusion adopted by the JHA Council at its meeting on 24-25 February "welcomes" the Commission's Communication and "strongly supports the aim outlined in the Communication according to which appropriate protection must be ensured for individuals in all circumstances." However, the document strongly emphasises the "specificities" of police and judicial cooperation in criminal matters and highlights the fact that a comprehensive approach "does not necessarily exclude specific rules" for this field, namely that "certain limitations have to be set regarding the rights of individuals" or "that

the powers of the data protection authorities should not interfere" with rules for criminal proceedings. [17]

The EDPS takes account of the specificities of the fields of policing and justice and does not rule out "special rules and derogations" in his Opinion, but he hopes that the data protection revision could mean that the future rules will also apply to domestic processing and that "D[ata] P[rotection] A[uthorities] will have the same extensive and harmonised powers vis-à-vis police and judicial authorities as they have vis-à-vis other data controllers." Moreover, the EDPS recalls that "limitations to the rights of data subjects...have not to alter the essential elements of the right itself." Therefore, he demanded special safeguards as compensation for data subjects, (e.g. to distinguish between "data based on facts" and "data based on opinions or personal assessment," to distinguish between the data of suspects and non-suspects such as witnesses, victims or suspects' contacts). [18] The Council's Conclusion does not contain a single word on such safeguards.

Europol's vision

Meanwhile work on "priority actions" to implement the Information Management Strategy is progressing slowly but steadily (see Table 2 for the IMS's action list). The European Police Office (Europol) has become a key player in this process, leading four of the 11 actions: firstly, Europol has become the senior partner with Spain in the project for an "Information Exchange Platform for Law Enforcement Agencies" (IXP); secondly, it is collaborating closely with Germany in an initiative which aims to refine the "Universal Message Format" (UMF) for standardised data exchange; thirdly, the agency is coordinating efforts to develop standards and guidelines for the management of information exchange in the field of law enforcement and, fourthly, it is drafting a definition of the "target information management architecture" for 2015. [19]

Plans for the IXP were first unveiled in January 2010 by the Spanish EU Presidency. Europol's draft "business concept" presented at a meeting of the DAPIX Working Party in June 2010 explains that the goal of the project is to target end-users including "local, regional and national police forces, customs, coast guard and border control authorities", "international law enforcement bodies, like FRONTEX, OLAF, Interpol, EMCDDA, CEPOL, EuroJust and Europol" and possibly "other institutions, such as DG JLS, the Council Secretariat General, but also judicial, prosecution and penitentiary services" and even third countries like "Norway, Iceland, Liechtenstein and Switzerland".

Envisaged as a "single website that serves as the starting point for any products or service related to international law enforcement cooperation", the platform should "facilitate smooth access" to relevant legislation, policy documents, forms, tutorials, details on national and EU law enforcement structures etc., and it should make available "tools" for data mining, monitoring of the internet or open source consultation. The IXP should also provide a meta-search engine that "processes queries across the relevant databases managed in the framework of justice, liberty and security, and potentially also national databases." Reference is made to related plans for a European Police Records Index System (EPRIS) which suggests that the search function works on the basis of an index. This indicates that searched information is held by other agencies without making them fully available. The IXP should also link to "the communication channels used for cross-border information exchange, such as Interpol I24/7, SIRENE and the Europol communication tool SIENA". [20]

The objective of the "Universal Message Format" is to develop and upgrade communication channels. The project started some years ago at the initiative of Sweden, Germany, the

Netherlands and Europol and it is aiming to develop a prototype of a standardised format for electronic information exchange under the "Swedish Initiative", Council Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities. [21] Its first results were presented in 2009. [22] The objective of the IMS is now to refine the prototype by defining an information model "suitable for all cases of police information exchange within Europe" from which the technical specifications of a UMF II can be derived. Following this, the new message format will be promoted and institutionalised and eventually made universal by making its use binding. [23] Though it remains to be seen whether the manifold "languages" of policing across Europe can be translated into a standardised message format, countries like Belgium, Bulgaria, Greece, Hungary, and the United Kingdom have already expressed their interest in such harmonisation. [24] In addition, Norway, Switzerland, Iceland, Liechtenstein, the EU border agency Frontex, the EU anti-fraud office Olaf, Eurojust and even Interpol have been invited to join the process. [25]

The technical and semantic convergence sought by the promotion of UMF II will be bolstered by organisational harmonisation. The objective of the third IMS action led by Europol is to develop and test standards and guidelines for the management of information exchange instruments. The theoretical part of this exercise was reported to have been concluded in autumn 2010 and should be followed by a practical demonstration using Europol's "Secure Information Exchange Network Application" (SIENA) as a test bed. [26] SIENA replaced the older Europol communication system InfoEx in 2009. What is new is that SIENA not only connects Europol and the National Liaison Officers at The Hague, but also aims to integrate Europol National Units (ENU) within the Member States and eventually establish direct interfaces with national information systems. [27] Given the emerging expansion of Europol's electronic communication channels, it is crucial for the agency to establish at least minimal common standards for SIENA across Europe. Moreover, information exchange via SIENA is a litmus test for Europol's capability to manage and exploit future initiatives in information exchange.

Europol has announced that it will publish its vision of Europe's future information exchange architecture in July 2011. Informed by the European Commission's mapping exercise, the agency, supported by Finland, will then outline the "desired state of the information landscape by 2015". [28] It is already clear that Europol is anxious to establish itself as the "EU criminal information hub" and "one stop shop for data exchange and matching". [29] But what role will the protection of privacy and personal data play?

A victim of the crisis

Flanked by the promises made in the Stockholm Programme, the Lisbon Treaty and the Charter of Fundamental Rights, and by a rising awareness of the digital vulnerability of individuals in the information age, data protection has made some inroads in the areas of police and justice. Europol and Spain's ambitious plans for the IXP, for instance, have been criticised by the DAPIX data protection subgroup and also questioned by other members of the Working Party. The team in charge of defining "interoperability" raised the question of whether the term could simply be treated as a technical issue without any relevance to issues of data protection. [30] Each proposal made in the context of the IMS action list makes at least rhetorical reference to data protection: a definition of access rights, roles and logfiles are demanded for information exchange instruments. The Council's response to the Commission's Communication on the comprehensive approach to data protection recognises compliance with the principles of necessity and proportionality as preconditions for the exchange of personal data in police and judicial cooperation.

However, when it comes to implementation the reality is less promising. Priority action number 2 of the IMS action list is the development of a so-called "Data Protection Impact Assessment toolkit," the objective of which is to "ensure that information exchange is fully compliant with fundamental rights." Chaired by the United Kingdom, the project group set out in summer 2010 to collect examples of "good practice" and produce "robust arguments" for the use of Data Protection Impact Assessments (DPIAs) in order to engage other Member States and produce guidance. A lack of interest by the DAPIX Working Party was seen as the highest risk to the success of this activity. [31] To foster the process, and reduce the burden on other Member States, the UK Ministry of Justice devoted two part-time staff to the project who collected examples for DPIAs from the Anglophone world. [32] The DAPIX meeting was informed on 20 December 2010 that Estonia had joined the project group. The bad news was: "On the substance, however, little progress had made in particular against the backdrop of considerable national budget cuts." [33] Obviously other priorities overshadowed the IMS "priority action" devoted to the protection of fundamental rights.

This Analysis first appeared in *Statewatch Journal* Vol 21 no 1

Footnotes

1. Council doc. 16637/09, 25.11.09
2. Council doc. 11312/09, 26.6.09
3. Council doc. 13972/09, 19.10.09
4. Council doc. 16951/1/09, 18.1.10
5. Council doc. 6660/10, 2.3.10
6. COM (2010) 385 final
7. COM (2010) 606 final, 4.11.10
8. EDPS press releases, 30.9.10 and 15.11.10
9. Less than five per cent of the Prüm "hits" (249 of 5160 cases) between Germany and Austria, Spain, Luxemburg, the Netherlands and Slovenia occurred during investigations of serious crimes until October 2009. German Parliament doc. BT 16/14150, 22.10.09.
10. De Hert, P. / Vagelis P.: The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters. A modest achievement however not the improvement some have hoped for. In: Computer Law & Security Review 25: pp. 403–414.
11. Council doc. 16918/10, 2-3.12.10
12. Council doc. 18190/10, 22.12.10
13. Council doc. 17923/10, 10.1.11
14. Council doc. 5366/11; presented by the EDPS at the DAPIX subgroup meeting on 17.1.11.
15. Council doc. 5980/11, 1.2.11
16. Council of German States doc. Bundesrat Drucksache 707/10 (Beschluss), 11.2.11
17. Council doc. 5980/4/11, 15.2.11
18. Council doc. 5366/11, 17.1.11, pp. 45-47
19. Council doc. 11125/10, 15.6.10
20. Council doc. 11117/10, 15.6.10
21. http://www.semic.eu/semic/view/snav/network/Communities/UMF.xhtml
22. D. Borchers: Europäischer Polizeikongress. You Parlez UMF? 12.2.09. http://www.heise.de/security/meldung/Europaeischer-Polizeikongress-You-Parlez-UMF-Update-194851.html

23. http://www.semic.eu/semic/view/documents/semic-community-umf-roadmap.pdf
24. Council doc. 11125/10, 15.6.10
25. Council doc. 11087/10, 15.10.10
26. Council doc. 11125/10, 15.6.10
27. Baden-Württemberg Ministry of Interior: Bericht des deutschen Ländervertreters im Ausschuss nach Artikel 36 EUV über die Beteiligung der Angelegeneheiten der Europäischen Union. [Report of the Representative of the German States at CATS]. Stuttgart. 30.3.10, p. 16
28. Council doc. 15198/10, 20.10.10
29. Council doc. 6517/10, 22.2.10
30. Council doc. 11353/10, 21.6.10
31. Council doc. 11817/1/10, 19.10.10
32. Council doc. 14458/10, 18.10.10
33. Council doc. 18190/10, 22.10.10