COM(2010)385
12579/10

EXPLANATORY MEMORANDUM ON EUROPEAN UNION DOCUMENT

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT – OVERVIEW OF INFORMATION MANAGEMENT IN THE AREA OF FREEDOM, SECURITY AND JUSTICE

Submitted by the Home Office on August 9 2010

SUBJECT MATTER

1. This Communication presents, for the first time, a full overview of the EU-level measures in place, under implementation or under consideration that regulate the collection, storage or cross-border exchange of information for justice and home affairs. It is the first step in delivering the Stockholm Programme objectives to create an information system architecture that will help to improve the exchange of information between European police forces; yet also give citizens the right to know what personal data is processed and exchanged about them, by whom and for what purpose. It is also the first time that the Commission has presented its vision of the broad principles that it intends to follow in the future development of EU instruments for the collection, storage or exchange of data.

2. Twenty five EU data exchange mechanisms have been included, along with several EU data exchange platforms (the underlying system structures). They have only looked at data exchange systems which contain personal data. Each data exchange mechanism has been examined to identify the proposer, purpose, structure, personal data coverage, authorities with access to the data, data protection provisions, data retention rules, state of implementation, and review mechanism. A comprehensive background and history has been produced for each of the twenty five mechanisms.

3. The existing EU data exchange mechanisms examined are:
    - Schengen Information System (SIS)
    - Second-generation Schengen Information System (SISII)
    - Eurodac
    - Visa Information System (VIS)
    - Advance Passenger Information (API)
    - Naples II Convention
    - Customs Information System (CIS)
    - Customs file identification database (FIDE)
    - Swedish initiative
    - Prüm Decision
    - Data Retention Directive
    - European Criminal Records Information System (ECRIS)
    - Financial Intelligence Units (FIUs)
    - Asset Recovery Offices (AROs)
    - Cybercrime Alert Platforms
    - European Police Office (Europol)
    - European Union's Judicial Cooperation Unit (Eurojust)
    - Passenger Name Records (PNR)
    - Terrorist Finance Tracking program (TFTP)

4. EU data exchange mechanisms suggested in the Stockholm Programme Action Plan and examined in this Communication are:
    - Passenger Name Records package
    - Entry/Exit System (EES)
    - Registered Travellers Programme (RTP)
    - EU terrorist finance tracking system
    - Electronic System of Travel Authorisation (ESTA)
    - European Police Records Index System (EPRIS)

5. The Communication outlines that there are eight significant observations from this review. These are:

6. **Decentralised structure**: Only six of the data exchange mechanisms examined involve the collection and storage of personal data on databases. These are SIS (and SISII), VIS, EURODAC, CIS, Europol and Eurojust. The IT Agency proposals already aim to take on the operational management of these databases. The remainder regulate the exchange of data held nationally and the EU seeks to add value by enabling the exchange of such information under certain circumstances.

7. **Limited purpose**: Purpose limitation appears to be a core factor in the design of EU-level information management measures.

8. **Potential overlaps in function**: Purpose limitation means that personal data is collected via several different instruments separately and is processed separately. An individual's name, date and place of birth and nationality are duplicated in the majority of systems. Biometric data, such as fingerprints or photographs, and other highly specialised personal information are all gathered independently for each mechanism. Alternatively mechanisms revert to bilateral contacts, often without EU level requests. Only the Swedish initiative would be sufficient in legal terms to exchange any type of data for investigations (subject to national law permissions), while the Prüm Decision is the preferable practical mechanism from an operational perspective.

9. **Controlled access rights**: In line with the purpose limitation, the right to access is triggered by the nature of the measure. The flow of information is controlled by the national interfaces, national contact points or central coordinating units specifically set up for that mechanism.

10. **Variable data retention rules**: Retention periods vary widely depending on the objectives of the various instruments. The concept of active and passive data may also be a decision factor.

11. **Effective identity management**: Several measures, but specifically SISII and VIS, aim to allow identity verification through the use of biometric data.

12. **Data security via EU solutions**: Several instruments of varying size, structure and purpose rely on the Commission-funded s-TESTA data communication network for sharing sensitive information. Europol's SIENA information exchange network application seems to have become the other application of choice.

13. **Divergent review mechanisms**: The range of review mechanisms employed suggests that the current structure of information management in the EU is not conductive to the adoption of a single evaluation mechanism for all

instruments. Therefore it is essential that any future amendment of any instrument in the field of information management also takes account of its potential impact on all the other measures.

14. As a result of this review, the Commission has identified two sets of core principles that should be applied to all existing and future EU JHA data exchange work, including new specific proposals. They suggest that this benchmark will guide initiation and evaluation of policy proposals across the breadth of work in the area of freedom, security and justice, in order that new ideas and review of the existing body of legislation are complementary and follow the general principles laid down in the EU Treaties. These are:

15. **Safeguarding fundamental rights, in particular the right to privacy and data protection:** When developing new instruments that rely on the use of information technology, the Commission will apply a 'privacy by design' approach, to embed personal data protection in the technological basis of the proposed instrument so that data processing is limited to a 'need to know' basis.

16. **Necessity:** In all future policy proposals, the Commission will assess the initiative's impact on individuals' right to privacy and personal data protection. They will set out that impact against three criteria; is it lawful, proportionate to the legitimate aim of maintaining internal security, and necessary.

17. **Subsidiarity:** Any new legislative proposal will contain a statement and assessment of need for a burden to fall on the EU, national governments, regional authorities, economic operators and citizens. In the case of new international agreements, this statement will also consider the proposal's expected impact on relations with third countries in question. This will make it possible to appraise compliance with the principle of subsidiarity in Article 5 of the Treaty on European Union.

18. **Accurate risk management:** Risks should be based on evidence and not be hypothetical. Risk linked to an individual's past behaviour or pattern of behaviour should be seen against necessity testing and purpose limitation, and the development of a risk profile which is compatible with fundamental rights is relevant.

19. **Cost-effectiveness:** In view of the current economic climate, all new proposals must be cost-effective. Establishment or upgrades will take account of pre-existing solutions to minimise overlap and to maximise possible synergies. This may include auxiliary functions to exiting information systems before proposing new systems if the Commission assesses that a proposal's objectives can be accomplished through better use of existing instruments.

20. **Bottom-up policy design:** The development of new initiatives must be based on consultation of stakeholders, so the Commission will establish permanent liaison with national officials and practitioners through Council structures, management committees and ad hoc formations..

21. **Clear allocation of responsibilities:** To avoid failures and delays in central delivery or unsupported decentralised implementation by Member States, the future IT Agency may be able to provide EU wide advice, a platform for stakeholder engagement, and safeguard against overruns and delays.

22. **Review and sunset clauses:** The Commission will review each instrument covered in this Communication, with the first reviews due by the end of 2010. Existing instruments will only be maintained if they continue to serve the legitimate purpose for which they were designed.

23. Additionally the Commission is conducting an 'information mapping' exercise on the legal bases and practical operations of the instruments. This will be presented to the Council and European Parliament in 2011, with a view to presenting a communication on the European Information Exchange Model in 2012.

SCRUTINY HISTORY

24. None, as this is a new Communication. However, the legislative proposals to create the existing EU measures were all subject to scrutiny prior to their adoption.

MINISTERIAL RESPONSIBILITY

25. Overall Justice and Home Affairs policy in England and Wales is a shared responsibility between the Home Secretary, the Secretary of State for Justice and the Attorney General. The Cabinet Secretary for Justice is responsible for Scotland and the Minister for Justice is responsible in Northern Ireland.

INTEREST OF THE DEVOLVED ADMINISTRATIONS

26. The devolved administrations have an interest in the issues in the Commission Communication, particularly in cases where police data exchange measures have to be implemented separately. The Scottish Government, Northern Ireland and Wales have been consulted in preparing this EM and are content.

LEGAL AND PROCEDURAL ISSUES

i) Legal basis

27. None for this Communication itself. However, any legislative proposals arising as a result of this Communication would in general fall within Title V TFEU.

ii) European Parliament procedure

28. The Communication is directed at the European Parliament for information. Legislative proposals arising from this Communication would follow the procedure appropriate to their legal base.

iii) Voting procedure in the Council

29. None. Legislative proposals arising as a result of this Communication would follow the procedure appropriate to their legal base.

iv) Impact on United Kingdom Law

30. None. Legislative proposals arising as a result of this Communication may have an impact on UK law.

v) Application to Gibraltar

31. None. Legislative proposals arising as a result of this Communication may be applied to Gibraltar.

vi) Fundamental Rights Analysis

32. Not applicable. A fundamental rights analysis is not required as this is not a legislative proposal.

APPLICATION TO THE EUROPEAN ECONOMIC AREA

33. None. Legislative proposals arising as a result of this Communication may apply to the European Economic Area.

SUBSIDIARITY

34. No issues of subsidiarity arise from this Communication itself, although any individual legislative proposals arising as a result of this Communication would need to be considered separately.

POLICY IMPLICATIONS

35. The Government welcomes the Commission Communication as the first review of its kind detailing all EU data sharing mechanisms in the Justice and Home Affairs area.

36. The Stockholm Programme objectives are an important basis to work from. Information exchange is not an end in itself but a means of working towards providing greater public good - in combating crime, in facilitating legitimate travel, in doing business abroad, and in managing identity. But it is important to strike the correct balance between private and public interests. Effective data protection must be a prerequisite for information sharing, along with transparency about the collection, retention, and use of personal information.

37. The UK has continued to advocate the creation of internal EU rules for the collection and sharing of PNR data as foreseen on page 20 of the Communication. At the July informal Justice and Home Affairs Council the UK expressed disappointment at the Commission's proposed timetable for introducing this, noting the role of Passenger Name Records in fighting organised crime. We believe that a 2011 date for publication is too late and are actively encouraging the Commission to bring this forward to this year.

38. The UK would not expect to participate in the new proposals foreseen for and Entry/Exit System (EES); Registered Travellers Programme (RTP) or Electronic System of Travel Authorisation (ESTA) since they are likely to build on that part of the Schengen acquis in which we do not participate. The UK has chosen to maintain its own frontier controls and therefore does not participate in those elements of the Schengen acquis which regulate entry into the Schengen area, maintaining our own visa arrangements for third country nationals.

39. We would want clear evidence of the added value of an EPRIS over and above the existing systems such as the Swedish initiative, which already provides for the exchange of information for police purposes.

40. The guiding principles proposed by the Commission seem uncontentious. Proportionality and subsidiarity are Treaty requirements for any new initiative. We would always expect a cost assessment to accompany any new proposal. Necessity has also been a principle advocated by the Government in the development of EU measures.

41. Our considerations of any existing or future initiatives in this field would include:
    - The necessity and overlap of systems in operation, planned or proposed at EU level and their practical application in the UK.
    - The impact on UK system structures where they mirror EU systems.

- The benefits and risks of centralised and decentralised systems, including the base applications used and control rights granted.
- Data retention and data protection.
- How best to review an existing or proposed mechanism against another.
- The impact on Member State right of initiative, bilateral agreements and cooperation, and international agreements.
- The benefits and risks of profiling.
- Best practice on cost-effectiveness and engaged policy development.
- The role of the IT Agency in the context of this review; and
- The impact of any future changes to the purpose or functionality of existing EU data exchange legislation, including the use of repeal and replace proposals and the resulting impacts on UK participation and opt-in.

42. This Communication is not legislative and the UK opt-in does not apply.

IMPACT ASSESSMENT

43. An Impact Assessment (IA) is not required on this Communication itself. IAs may be required on legislative proposals arising as a result of this Communication. These would need to be considered separately.

FINANCIAL IMPLICATIONS

44. None for this Communication itself. Any legislative proposals arising as a result of this Communication would need to be considered separately.

CONSULTATION

45. Due to the wide ranging nature of this Communication, the Government position has been prepared in consultation across Whitehall, associated agencies, the devolved administrations and relevant stakeholders.

TIMETABLE

46. The Communication has not yet been formally presented to Justice and Home Affairs Ministers. This may take place on 7 October 2010. The European Parliament has yet to set its timetable for consideration. Council working group level discussions on individual EU data exchange mechanisms will recommence in mid September, as will Commission and Member State work on the 'information mapping' exercise and police information models.

DAMIAN GREEN
Minister for Immigration
HOME OFFICE