



JUSTICE

**Comments requested by the
Department for Constitutional Affairs
on the EU Draft Council Framework Decision
on the protection of personal data processed
in the framework of police and judicial co-operation
in criminal matters**

February 2006

**For further information contact:
Maik Martin, Legal Officer (EU Criminal Justice)
Tel: (020) 7762 6433 Email: mmartin@justice.org.uk**

Introduction

1. JUSTICE is an independent all-party law reform and human rights organisation, which aims to improve British justice through law reform and policy work, publications and training. It is the UK section of the International Commission of Jurists.
2. We are grateful for the opportunity to comment on the proposal for an EU Council Framework Decision on the protection of personal data in the framework of police and judicial co-operation in criminal matters. While wishing to emphasise certain aspects and shortcomings of the proposal (which we are aware may still change considerable during the Council negotiations), JUSTICE fully endorses the European Data Protection Supervisor's opinion of 19 December 2005 on this matter.

Key observations

3. JUSTICE welcomes the proposed adoption of an instrument providing for the protection of personal data processed in the course of police and judicial co-operation under the EU Treaty's Third Pillar, complementing the Data Protection Directive 95/46/EC and fleshing out the rights to respect for privacy and protection of personal data as laid down in art 8 ECHR and arts 7 and 8 of the EU Charter of Fundamental Rights.
4. We consider a high level of data protection to be an indispensable prerequisite for measures to be adopted under the Third Pillar for the facilitation and improvement of intra-EU data exchange in the areas of police and criminal justice co-operation.
5. Provided its timely and correct implementation, we believe the present Commission proposal for a Framework Decision (FD) to afford EU citizens a high degree of protection of their personal data. In particular, we welcome the wide scope of the proposed FD in that its general principles will be applicable to both domestic and cross border data processing. We also consider the provisions in Title VI of the TEU to provide the proper legal basis for an instrument of such scope.
6. However, we regret that

- The proposal does not set up a comprehensive data protection *regime* also covering Third Pillar or EU convention institutions such as Eurojust and Europol;
 - The FD does not address the problem of the transmission of domestically collected personal data to third countries and therefore does not provide for restrictions on data transmission reflecting the adequacy of data protection levels in individual third countries;
 - The FD does not address the issue of the quality and accuracy, and verification thereof, of personal data received by Member States from third countries;
 - Strict time limits for data storage have effectively been left to the Member States to lay down without providing for any meaningful framework limiting this competence in art 7(1) of the FD;
 - The definition of legitimate purposes for the processing of personal data in the police and criminal justice context throughout the FD (eg in arts 7(1), 9(7) last indent, 11(1)(a), 12(c)) is unduly vague and may thus offer only little guidance and protection for data subjects in practice;
 - The differentiation between categories of data subjects according to their role in police and criminal justice proceedings in art 4(3) of the FD is not reflected sufficiently in the provisions on safeguards for personal data of those subjects;
 - The special nature of DNA data is not addressed in the FD; DNA data is not defined as special category of data under art 6(1) of the FD;
 - The determination of adequacy of data protection levels in third countries through the procedure provided for in art 16 of the FD opens up the assessment to extraneous political considerations and does not give the envisaged art 31 working party enough say in this matter.
7. Criticism has been levelled at the proposed FD - in particular its stringent requirements for data accuracy verifying, logging and transmission documentation – for causing an unacceptable increase in the administrative workload of police and criminal justice agencies engaged in data processing. JUSTICE firmly believes, however, that an increase in workload, which may result from member states complying with the proposed FD, will be adequately compensated by the dramatic facilitation of the procedures for intra-EU data exchange as envisaged by the proposed FD on data exchange under the principle of availability.

8. **JUSTICE therefore believes that the proposed FD should be adopted while consideration should also be given to the remarks set out below.**

The need for a Third Pillar data protection instrument

9. The process of creating an area of freedom, security and justice within the EU entails an ever closer co-operation between member states' organs in the law enforcement and criminal justice system. This increased co-operation will require a new system for swift intra-EU exchange of data relevant for law enforcement purposes. While JUSTICE has reservations on certain aspects of the Commission proposals both for a FD on the exchange of information under the principle of availability (COM(2005) 490) and for a FD on the organisation and content of the exchange of information extracted from criminal records between member states (COM(2005) 690), it is obvious that improvement of information exchange mechanism on all levels will be essential for the achievement of an area for freedom, security and justice. However, increased data exchange, in turn, calls for an adequate level of protection of personal data under the Third Pillar as it will inevitably greatly affect the EU citizens' right to data protection as guaranteed in arts 8 of both the ECHR and the EU Charter of Fundamental Rights.
10. The present proposal for a FD, having been drafted closely along the lines of the 1995 EC Data Protection Directive, will generally ensure a high standard of protection of sensitive personal data in the area of police and criminal justice co-operation. However, JUSTICE sees then need to highlight a number of aspects of the proposal that would need further discussion and improvement.

A sufficient legal basis for the proposed FD

11. First and foremost, we believe that the TEU, in particular its art 31(1)(c), provides a sufficient legal basis for provisions covering not just the conditions for transmission of personal data between member states *simpliciter* but also the way personal data in national police and criminal justice databases should be processed, thus laying down certain minimum rules and principles applicable also to data processing within the member states.
12. Such relatively comprehensive regulation of data processing standards in member states is consistent with art 31(1)(c) TEU. Cross border transmission of personal data

cannot be regulated adequately without approximation of safeguards and standards governing the domestic processing of data: where personal data are made available between member states by direct automated access with only an extremely limited scope for case-by-case pre-transmission verification of data accuracy, ensuring data accuracy and fair processing of data in general at member state level is imperative. In that sense the proposed FD is indeed ensuring compatibility of member states' data protection laws in order to improve police and judicial co-operation in criminal matters. This is recognised in recitals 7, 8 and 9 of the proposed FD.

The need for an overarching data protection instrument in the Third Pillar

13. In light of the proposal for a FD on the organisation and content of the exchange of information extracted from criminal records between member states JUSTICE welcomes that the present FD proposal not only covers data exchange between police and law enforcement agencies but also encompasses data on criminal prosecutions and the consequences thereof.

14. However, we regret that the proposed FD does not contain provisions extending the scope of the FD to both Europol and Eurojust. While separate data protection provisions are already in place for these bodies, it would be desirable to regulate all Third Pillar data protection issues in one comprehensive instrument, which, due to the legal nature of framework decisions as being addressed to member states exclusively, would have to be of a hybrid legal nature.

Addressing third country data exchange comprehensively

15. JUSTICE is very concerned about the lack in the present proposal of provisions governing the transfer *simpliciter* of data processed in a member state to third countries. While art 15 of the FD addresses the issue of *further* transmission of personal data to third countries (ie of data received by one member state from another and then made available to third countries), no provision is made for situations where data are made available to a third country by the member state which had previously gathered them. **As the origin of personal data has no bearing on the risk of those data being given only inadequate protection in third countries, the restriction of third country data transfer in art 15 of the FD should be extended to cover data transmission *simpliciter* to third countries as well.** Art 31(1)(c) TEU would provide sufficient legal basis for such a clause.

16. **Equally, we regret the absence of provisions regulating and restricting the use of personal data received by a member state from a third country.** While it has to be acknowledged that verification of accuracy and quality of data gathered and processed in a foreign country will be formidably difficult, safeguards will still have to be put in place to prevent data collected and further processed incompatibly with human rights standards and basic standards of data protection from being processed by member states. Taking the example of personal data obtained by a third country government through illegal activities such as torture, rules have to be adopted prohibiting the processing by member states of data made available by third countries without any prior assessment of the third country's compliance with adequate human rights standards. Moreover, we would argue that data obtained through torture in a third country must under no circumstances be processed by a member state.

Adopting a stricter framework for member states' data processing laws

17. JUSTICE considers some of the limits and criteria for member states' data protection legislation laid down in the FD to be unhelpfully vague and overly broad. In particular, the time limit provision in art 7(1) of the FD has to be regarded as insufficient in two respects:
18. Firstly, while stating that personal data may only be stored as long as it is necessary for the purpose for which they were collected, the clause then goes on to give member states' legislatures *carte blanche* in extending this purpose-oriented time limit at will. Any guidance or limits as to how far member states may actually go in setting time limits for data processing are entirely missing.
19. Secondly, even the envisaged time limit for data storage using the purpose criterion is an unhelpfully vague one. In criminal proceedings personal data will, as a rule, have been collected for the purpose of investigating and prosecuting a specific criminal offence. Once the proceedings have been completed by conviction or acquittal of the defendant, the personal data of those implicated in the proceedings are as such no longer needed. The initial purpose for collecting these data is fulfilled, so that no further processing of these data would be allowed. If, however, it would be argued that even the initial data collection process also served the purpose of crime reduction and improving the work of the police and law enforcement agencies in fighting crime *in general*, there would hardly be any definite time limit for processing

these data even after initial criminal proceedings have been completed. Personal data could then be stored for an indefinite time as they could theoretically always be used to facilitate criminal investigations in the future.

20. In this context it also remains unclear whether there is an intended difference in meaning between the term “purpose” in art 7(1) and the term “specific purpose” in arts 11(1)(a) and 12(c) of the FD.

21. We therefore recommend to provide, in the FD, for clear and unambiguous time limits and purpose limitations for the processing of personal data to be legitimate.

22. With regard to the criteria for the necessity of the processing of personal data as laid down in art 4(4) of the FD, we would like to remark that we consider the first limb of the three pronged test to be very wide (“facilitate or accelerate”). However, taking into account the two further limbs of the test, in particular the third limb (proportionality), we hold the view, albeit with some hesitation, that this test will conform to art 8 of both the ECHR and the EU Charter of Fundamental Rights.

A difference in treatment for different categories of data subjects and sensitive data

23. JUSTICE welcomes the differentiation in art 4(3) of the FD between the data of different categories of data subjects implicated in the criminal justice process in the broader sense. We regret, however, that this differentiation remains largely inconsequential in that of the whole FD only the last sentence of art 7(1) refers to it. **We believe that this distinction is crucial in the area of criminal justice data processing and should be reflected in the level of protection of personal data according to the individual degree of implication in criminal proceedings.**

24. Equally, we are concerned that amongst the categories of particularly sensitive personal data listed exhaustively in art 6(1) of the FD, there is no mentioning of DNA data. With regard the most recent worrying experience in the UK with a speedily growing police DNA database comprising personal data of individuals who have never even been charged with, or cautioned for, a criminal offence, **JUSTICE strongly urges for the inclusion of DNA data as another special category of data within the meaning of art 6(1) of the FD.**

Depoliticising the third country adequacy assessment procedure

25. While the procedure provided for in arts 15(4) and 16 of the proposed FD for the assessment of adequacy of third country data protection standards through the art 16 committee mirrors the provisions of the 1995 EC Data Protection Directive, we believe that a case can be made for the process to be depoliticised.

26. In the highly sensitive area of police and judicial co-operation in criminal matters, encompassing counter-terrorism law enforcement co-operation in a politically charged environment, we consider it essential that decisions on the adequacy of data protection levels in co-operating third countries should be taken out of the political arena as far as possible. **While recognising that it is primarily for the individual member state to make the appropriate determinations on data protection standards under art 15(2) of the FD, we think that the art 16 committee procedure should be revised so as to give the member states' data protection supervisory authorities and the EDPS a greater say in the decision on third country data protection adequacy.**

27. We believe that giving the art 31 working party of supervisory authorities a right to veto a decision taken under the art 16 procedure as presently envisaged, would, at least to a certain extent, limit the influence of purely political, extraneous reasons on the very important decision of adequacy of third country data protection standards. Such a veto could require a positive two-thirds majority of the art 31 working party members.

MAIK MARTIN
EU Criminal Justice Legal Officer
February 2006