COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

Recommendation Rec(2003)14
of the Committee of Ministers to member states
on the interoperability of information systems in the justice sector

(adopted by the Committee of Ministers on 9 September 2003
at the 851st meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity among its members;

Determined to improve the quality of public service to citizens and businesses in the justice sector;

Affirming that an efficient justice system is essential to consolidate democracy and strengthen the rule of law, as it will increase public trust and confidence in the state authority, in particular its ability to fight against crime and solve legal conflicts;

Recognising that information technology has become indispensable for efficient functioning of the justice system, especially in the light of the increasing workload of the courts and other justice sector organisations;

Recognising that efficient functioning of the justice sector in the information age requires legal recognition and wide use of electronic data exchanges between different organisations;

Bearing in mind that constitutional, legal and administrative requirements and traditions entail the existence of a large diversity of information systems in the justice sectors of member states;

Aware of the growing complexity of information systems in the justice sector;

Realising that efficient and secure electronic data exchanges among different justice sector organisations in these conditions require interoperability of their information systems;

Recognising the potential of interoperability for facilitating transborder legal co-operation to meet the increasing practical need for closer co-operation between countries in the justice sector;

Aware of the various interoperability problems of information systems in the justice sector resulting from administrative, management and technical deficiencies;

Recognising the need to improve the interoperability of information systems in the justice sector by applying interoperable document and communication standards and integrated approaches to information technology projects;

Recognising that the introduction of interoperability in the justice sector requires also appropriate changes to the relevant law and work processes and adequate training of personnel;

Bearing in mind that interoperability solutions for the justice sector should be adapted to the specific requirements of member states;

Recognising the existence of varying interoperability needs of member states resulting from their differences regarding the development of information technology in the justice sector;

Recalling that changes in the work processes of justice sector organisations introduced by the interoperability should in no way affect the constitutional guarantees of the independence of the judiciary in the process of the administration of justice;

Aware that data processing in the conditions of interoperability presents both advantages and risks with regard to information security and protection of privacy in the justice sector;

Having regard to Recommendation Rec(2001)2 concerning the design and redesign of court systems and legal information systems in a cost-effective manner, Recommendation Rec(2001)3 on the delivery of court and other legal services to the citizen through the use of new technologies and Recommendation Rec(2002)2 on access to official documents,

Recommends that governments of member states:

1. implement the principles and guidelines set out in this recommendation in their domestic law and practice;

2. bring these principles and guidelines to the attention of persons and institutions responsible for information technology and interoperability in the justice sector.

I. General provisions

1. Definitions

For the purposes of this recommendation:

– “justice sector organisations” shall comprise the courts, prosecution and other public and private institutions, such as the police, penitentiary systems, public registers, civil status authorities, lawyers, notaries as well as other public and private stakeholders that exchange data and information in the process of the administration of justice;

– “information systems” shall mean information technology systems used by justice sector organisations for electronic data processing, storage and exchange, such as case (workflow) management systems and databases;

– “interoperability” shall mean efficient and secure data and information exchanges among the information systems of justice sector organisations.

2. Objective

The objective of this recommendation is to facilitate the interoperability of information systems by laying down principles and guidelines for member states concerning steps and measures to be taken at the level of information technology policy, process design and technical architecture of data and information in the justice sector.

II. Policy issues

3. Interoperability strategy

3.1. Member states should ensure that information technology projects launched in the justice sector take into account the need to ensure interoperability of information systems among various justice sector organisations.

3.2. An information technology strategy for the justice sector should take into account *inter alia* the following:

– stage-by-stage computerisation of the justice system;
– the establishment of communications infrastructure, including e-mail facilities;
– the development of an integration strategy to allow for system-to-system communication;
– the harmonisation of information to the extent needed;
– the establishment of an integrated system for data collection and statistical analysis;
– the introduction of a common management information system;
– the establishment of common internal information registers;
– the development of standard software for databases.

3.3. Information technology projects in the justice sector should, therefore, be implemented in the framework of co-ordinated programmes allowing for consistent actions to be taken in various interconnected fields and among different stakeholders, thus assuring the appropriate co-ordination and financing.

3.4. The introduction of interoperability in the justice sector should be based on cost-efficiency considerations. The required level of interoperability in each particular case should be determined with due regard to the costs involved and expected benefits.

4. Non-technical security and personal data protection

4.1. Member states should implement interoperability of information systems in the justice sector, taking full account of the need to ensure the security of information and personal data protection as required by applicable international standards and national law.

4.2. Member states should take measures to determine the roles and responsibilities of personnel of justice sector organisations regarding the use of information technology applications. Justice sector organisations should ensure, in particular, that they inform their personnel of the relevant legislation and regulations which apply to the way information and data are handled within the justice sector.

4.3. Member states should provide for the establishment of audit or control points at relevant positions in the automated information and document flows inside and among the justice sector organisations.

5. Human resources

5.1. In the introduction of information technology, justice sector organisations should deploy the necessary human resources to make sound judgements on the proposed systems and services.

5.2. Justice sector organisations should be provided with qualified personnel in charge of their information systems to ensure the respect of integrity, availability, storage and identification of electronic documents and data processed by the organisation concerned.

5.3. Member states should take measures to promote the training of lawyers and other personnel of justice sector organisations in matters related to the application of information technology. Incentives for the personnel of justice sector organisations should be created to encourage them to use information technology applications in their daily work.

6. Interoperability between the public and the private sectors

6.1. Member states should promote methods of electronic exchanges between public justice sector information systems and those of private justice sector organisations such as lawyers and other stakeholders. Such data exchanges may only be carried out in accordance with international and national law.

6.2. Member states should, at the same time, consider and implement appropriate precautions to ensure information security and personal data protection. Systems of accountability should be established in order to be able to control how information subject to special protection is handled.

III. Redefining the process design

7. Changes to work processes

7.1. To obtain maximum benefits from the introduction of information technology, member states should link the introduction of modern information technology in the justice sector to organisational changes to work processes of justice sector organisations.

7.2. Member states should have an open-minded approach to modernising laws and regulations where they constrain the use of opportunities made available by the new information technologies and, in particular, interoperability.

7.3. Introduction of interoperability in the justice sector should, however, be a controlled process. Member states should ensure that justice sector organisations identify, document and describe their work processes and monitor and control the changes introduced by interoperability.

8. Interorganisational process chains

8.1. Member states should apply interoperability solutions to all relevant fields where the interinstitutional co-operation of individual justice sector organisations is vital, such as criminal and civil justice systems.

8.2. Case management systems of justice sector organisations should, in particular, be prepared for delivering and receiving information from other external case management systems and providing support in the decision-making process by enabling access to a complete range of relevant databases.

8.3. Member states should facilitate the interoperability of various databases by introducing such unifying measures as unique identification codes and uniform data definitions.

IV. Technical and information architecture

9. Document and communication standards

9.1. Member states should adopt an integrated approach to the introduction of document and communications standards in the justice sector to enable data to be assembled in an agreed and structured way.

9.2. Interoperability can nevertheless be achieved by using more than one data standard since the adoption of a single standard may not be always possible. In this respect, member states should follow the development of the leading market *de facto* standards rather than attempt to create distinct standards for the justice sector.

9.3. In particular, member states should pay attention to the development of mark-up languages as promising emerging document and communication standards in the justice sector.

10. Technical security

10.1. Justice sector organisations should establish procedures to monitor and control potential exposure to risks arising from the misuse or failure of their information systems. These procedures should include security guidelines ensuring control of access to the various levels of their information systems.

10.2. Member states should, where appropriate, promote the application of cryptography in the justice sector to address some of the risks inherent in the digital media to secure electronic communications between various justice sector organisations.

10.3. Member states should also widely implement Public Key Infrastructure with respect to the justice sector organisations to ensure message integrity and non-repudiation as well as confidentiality through the ability to authenticate the recipient or sender of the message and verify electronic signatures with electronic certificates issued by trusted intermediaries.