# Mandate/ 289 EN

**Mandate addressed to CEN, CENELEC and ETSI in the field of Information Society Standardization**

## 1 Title

Mandate addressed to CEN, CENELEC and ETSI in support of the European Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995).

## 2 Rationale

The rapid and effective development of information society services is seen as a major element in global business and for job creation. Users and consumers will be able to search globally for goods and services they want at the price they are prepared to pay; there will be an almost unlimited choice. The provision of tailor- made services will be facilitated by technology that allows to gather information about the customer in an unprecedented way. However, users and consumers may not be ready to engage easily in this new electronic form of commerce if their right to privacy would be put at risk by undesired collection and further use of personal data. It is thus essential to ensure trust and confidence in the way personal data is dealt with by all actors including the use of specific electronic tools. A balance has been established by the European data protection Directives between commercial interest and the fundamental rights of individuals to privacy, in particular with respect to the undesired collection of personal data and the protection against abuses from the processing of personal data.

Until now, differences between national data protection laws have created potential risks of impeding on the exchange of personal data between Member States. The Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data (Directive 95/46) establishes a clear and predictable regulatory framework intended to provide both a high level of protection for the privacy of individuals in the Member States and as the free movement of personal data within the European Union. By fostering consumer confidence and harmonizing between Member States' data protection rules, the Directive will facilitate the further development of electronic commerce. The Directive lays down common rules to be observed by those who collect, hold, communicate or otherwise process personal data as a part of their economic or administrative activities or in the course of the related activities of their association. A potential role for the standards community in support of the implementation of the Directive can be seen at the following levels:

- Article 27 of the Directive invites the Commission and Member States to encourage the drawing up of codes of conduct both at national and European level. The objective is to complement and specify the provisions implementing the Directive in specific sectors and thus contributing to the harmonised implementation of the Directive. The Working Party set up by Article 29 of the Directive has the task to determine whether such codes of conduct are acceptable with regard to the requirements of national law implementing the Directive, in particular whether they provide added value and can be used in order to proof compliance. Guidance material prepared within the open consensus environment offered by European Standardization Organisations could be used as a "point of reference" for the elaboration of sector-specific codes of conduct and organisational schemes, and such specific codes of conduct could also be drawn up within that environment.

- The Directive is technology neutral, and applies to any form of personal data processing, be it manual or automated. However, the principle of data minimisation expressed in Article 6 of the Directive is the basis for the concept of "privacy enhancing technologies" which aims at organising the design of ICT technologies, systems and applications with a view to minimising the use of personal data in the functioning of technologies, systems and applications as such as well as in the provision of services using them. The standardization environment could play a role in testing and validating the conformity of such privacy enhancing technologies with the legal requirements of the Directive.

- Chapter IV of the Directive 95/46 allows for third countries with an adequate level of protection to receive personal data from the EU without further guarantees; a range of activities has been initiated both bilaterally and multilaterally, aiming at establishing a level playing field for business on a global scale. International standards could minimize differences between different countries and approaches, thus reducing potential conflicts and facilitating the implementation of the Directive.

**Standardization in support of the legal framework**

The Directive provides the necessary flexibility, in relation to the three levels identified in § 2.2, for self-regulation mechanisms, which include standardization, to draw the appropriate codes of conduct in support of the implementation and to implement the Directive effectively with a minimum of costs and organisational frictions. For self-regulatory instruments to be considered as appropriate in the context of "adequate protection" defined by the Directive, they must ensure a binding effect and provide adequate safeguards if data are transferred to third countries. In addition, the self-regulation instrument must be transparent and include the basic content of core data-protection principles. Mechanisms have to be provided to ensure a good level of compliance. The instrument should provide support to the individual data subject faced with a problem involving the processing of its personal data and appropriate redress in cases of non-compliance must be foreseen.

The consensus platforms offered by European Standardization Organisations could provide an adequate basis for self-regulation as their activities are by definition a broad, transparent and voluntary consensus- building process, bringing together all the relevant players. This, however, requires an intense dialogue between industry, users, consumers and public authorities which still needs to be established at the European level and beyond.

In the specific case of protection of individuals with regard to processing their personal data and the free flow of such data, the role of the standards community in support of the implementation of the Directive can be considered at following levels:

- Codes of conduct: the Directive establishes a legal European framework, which defines also the scope for self-regulatory mechanisms. Whilst respecting the role of the Data protection Working Party regarding the acceptance of Community codes of conduct, standardization in an open Workshop environment could provide the sectors with a platform to draw up the codes. It could also assist the sectors in reaching a broader European consensus for codes established within a specific sector and it could assist the Working Party in identifying a coherent set of European codes of conduct with the view to avoid duplication and incompatibility amongst sectors at European and national level.

- Privacy-enhancing technologies: The role of European standardization in support of the development of such technologies should be evaluated. European standardization could provide a common understanding of the concept of privacy enhancing technologies to be used in support of the implementation of the Directive. While evaluating the role of standardization, due account should be taken of the requirements of concerned parties such as users, consumers, industry, data protection representatives for the design technologies, systems and applications as well as the services relying on them.

- International standards: The Directive has a clear rationale on the adequacy of protection for data sent outside the Union. Not all countries have legislation in place for this purpose nor will national or sectoral self–regulation or contractual clauses provide a solution in every case. There is, however, a global commitment to implementing the OECD guidelines on this issue and related industry-led discussions are currently ongoing at a global level.

  Japan and Canada have already published standards implementing the OECD guidelines. In this case, European standardization initiatives should consider the suitability of preparing a European contribution, taking into account the Japanese and Canadian work, with the view to further enhance international consensus building and to prepare a co-ordinated input towards ISO. Internationally agreed implementation guidelines complementing the OECD guidelines would provide a good basis for “adequacy of protection” in support of data flow outside the Union.

## 3 Scope of the Mandate

The first step is to provide an analysis and evaluation of the potential role of the European Standardization Organisations in support of the Directive 95/46/EC. In

particular European consensus platforms may contribute to a smooth implementation of the Directive in the Member States and improving the level of "data protection" in third countries, by supporting the development of codes of conduct and foster the development of privacy-enhancing technologies while responding to the need for a coherent system providing an adequate level of interoperability. The purpose of the Mandate is to support the implementation of Directive 95/46/EC, both within the EU as at international level. With respect to international initiatives the need arises to co-ordinate the European position in order to avoid frictions with the legal requirements as laid down by the Directive.

For this purpose, European Standardization organisations are invited to assess their role in support of the implementation of the Directive and to coordinate action in this field.

It should be clear that in assessing the role of standardization, organisations should be aware, as pointed out earlier in the Mandate, of the fast changing nature of global networks and the need to develop flexible, technologically neutral and competition enhancing solutions. As a consequence, it might well be the case that acceptable concensus products would be in the nature of guidance, codes of practice or other documents less then a formal standard, such as the examples on implementing the UK Data protection Act 1998 or similar NL codes of conduct.

## 4 Description of the mandated work

In preparation of a European standardization initiatives in support of Directive 95/76/EC efficient working methods are to be established with the view to include all relevant players and to provide close links with international related activities. Activities should be initiated in co-operation with industry, users and consumers, public authorities and representatives from other regions.

- First, CEN, CENELEC and ETSI are invited to establish, in close co-operation with all relevant players and as a basis for international co-operation, an open consensus-building platform on issues related to data protection and privacy.
- Secondly, CEN, CENELEC and ETSI, in co-operation with all relevant players, are requested to identify the potential role of their organisations in support of the requirements set by the Directive as described in the Mandate
- Thirdly, the European Standardization Organisations in co-operation with all relevant players, should identify and assess relevant work at international and European level, whether performed by formal standardization organisations or within other consensus platforms such as IETF and the WWW Forum, with the view to integrate these activities within a coherent strategy. Identification of further needs should result in the definition of a work programme, identifying further initiatives such as specifications, Workshops, or any other need for consensus.

## 5 Execution of the mandate

**5.1** Within three months of the date of acceptance of this mandate, CEN, CENELEC and ETSI shall present to the Commission a report setting out the arrangements they

have made for execution of this mandate. Particular attention shall be given to the involvement of all relevant parties and to the international dimension.

**5.2** CEN, CENELEC and ETSI are invited to create as soon as possible, an open European platform for data protection related standardization to promote consensus building in support of the three levels identified by the Directive.

.

**5.3** Within nine months of the acceptance of this mandate, CEN, CENELEC and ETSI shall present a report on the identification of future requirements in support of the European legal framework for data protection, taking into account the available work in this field.