Advice paper on special categories of data ("sensitive data")

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 06/036.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Table of contents

EXECUTIVE SUMMARY

This advice paper aims to assess the concept of "sensitive data" in Article 8 of the Data Protection Directive 95/46/EC. Article 8 defines sensitive data as personal data revealing racial origin, political opinions or religious or philosophical beliefs, trade-union membership and data concerning health or sex life. This advice paper provides an overview of how this concept of sensitive data is implemented in the EU Member States and gives examples of problems experienced by national supervisory authorities in applying this concept in practice. The advice paper in addition considers possible changes to the concept of sensitive data in the meaning of Directive 95/46/EC. In this respect, the Working Party discussed changes to the categories of sensitive data mentioned in Article 8 (1) of the Directive as well as to the exceptions in Article 8 (2) – (4), (5) and (7). Against the background of rapid scientific and technological developments it also considered whether the current approach to sensitive data – which is characterized by a conclusive list of data being regarded as sensitive per se – could be amended so as to react more flexibly to possible new forms of sensitive data or new forms of data and data processing which could lead to severe infringements of privacy.

The Working Party on the protection of individuals with regard to the processing of personal data

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure,

presents the following advice paper:

I. Introduction

The Data Protection Directive (95/46/EC[1]) and the Council of Europe Data Protection Convention of 1981[2] are based on the premise that certain categories of personal data, as distinct from all other personal data, require extra protection and may be processed by private and public bodies only for specific purposes and under special conditions.

The purpose of this advice paper by the Working Party is to analyse in greater detail the concept of "special categories of data" referred to in Art. 8 of Directive 95/46/EC, also known as "sensitive data".

To begin, existing regulations on sensitive data at the level of the Council of Europe, the European Union and the Member States are presented and their commonalities and differences are pointed out in order to show how this issue is handled in intergovernmental, EU and Member State law (II.1.-3.). Further, this advice paper focuses on concrete problems that have arisen in the Member States when applying the relevant national provisions implementing Art. 8 of the Directive (II.3.2.). The advice paper concludes by discussing possible regulatory changes to the current concept of sensitive data under Art. 8 of Directive 95/46/EC, both with respect to the data categories mentioned in Art. 8 (1) and the exceptions for processing in (2) – (4), (5) and (7) as well as the basic approach to sensitive data as such (III.).

II. Legislation concerning "sensitive data"

The rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "normal" personal data. Misuse of sensitive data, such as health data or sexual orientation (e.g. if publicly revealed), may be irreversible and have long-term consequences for the individual as well as his social environment. For this reason, the Convention and the Directive make the processing of data which by their nature are regarded

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23 November 1995, p. 31 ff.

[2] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ETS no. 108.

as sensitive dependent on certain safeguards and conditions, which go beyond the conditions for the processing of other personal data.

1. Art. 6 of the Council of Europe Data Protection Convention No. 108

Article 6 of the Council Convention No. 108 covers "special categories of data". These include personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life or criminal convictions.

Art. 6 prohibits automatic processing of such data "unless domestic law provides appropriate safeguards".

Under Art. 9 no. 2 of the Convention, exceptions to this prohibition may be allowed only when provided for by national law and when they constitute "a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others."

According to Article 11, the Convention sets only minimum standards for the processing of personal data, including the processing of special categories of data as defined in Art. 6, and parties to the Convention may derogate from these standards at national level.[3]

It is important to notice that the Convention neither defines the data categories nor the "safeguards" mentioned in Art. 6, thus leaving the parties significant discretion in this respect and thereby accepting the possibility of differences between national regulatory regimes.[4]

2. Art. 8 Directive 95/46/EC

With Art. 8 of the Data Protection Directive (95/46/EC), EU law contains an explicit provision on the processing of "special categories of personal data". Art.8 of the Directive sets out specific preconditions for the processing of sensitive data which apply in addition to the general rules on data processing in Art.6 and Art.7 of the Directive.

Art. 8 (1) of the Directive contains a general prohibition on processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Other than the categories "ethnic origin", "philosophical beliefs", "trade-union membership" and data concerning criminal convictions Art. 8 of the Directive thus covers the same types of sensitive data as Art. 6 of the Council of Europe Convention No. 108.

---

[3] Acc. to para. 48 of the Explanatory Report to the Convention, the contracting parties to the Convention may set higher standards of protection for additional categories of data "depending on the legal and sociological context in the country concerned", http://conventions.coe.int/Treaty/en/Reports/Html/108.htm.

[4] Compare Simitis, Revisiting Sensitive Data (1999), Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24-26 November 1999), with examples of differences between national provisions on sensitive data: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999.pdf .

The term “data *revealing* racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership” is to be understood that not only data which by its nature contains sensitive information is covered by this provision, but also data from which sensitive information with regard to an individual can be concluded.

Article 8 (2) – (4) of Directive 95/46/EC provides for specific exceptions from this prohibition. Under Art. 8 (2), sensitive data as defined in (1) may be processed under the following conditions: the data subject has given his explicit consent to the processing of those data (a); the processing is necessary for the purposes of carrying out the obligations of the controller in the field of employment law (b); the processing is necessary to protect the vital interests of the data subject or of another person (c); the processing is carried out in the course of legitimate activities by a non-profit-seeking body with a political, philosophical, religious or trade-union aim (d); or the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims (e).

Under Art. 8 (3), processing is allowed where it is “required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services”.

Art. 8 (4) contains a catch-all provision allowing the processing of sensitive data for reasons other than those mentioned in Art. 8 (2) “for reasons of substantial public interest (...) either by national law or by decision of the supervisory authority”. Recital 34 of the Directive lists as examples the areas of public health, social protection, scientific research and government statistics.

Art. 8 (5) is equally broad, stating that the “processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or subject to derogations under national provisions providing suitable specific safeguards”. Paragraph 5 thus represents an independent provision on the processing of data relating to offences, as such data – different from Art. 6 Council Convention No. 108 (above 1.) – are not regarded as sensitive data in the meaning of Art. 8 (1) and are thus not covered by the general prohibition on processing under (1).

Lastly, under Art. 8 (7) the Member States may “determine the conditions under which a national identification number or any other identifier of general application may be processed”. The processing of national identification numbers or similar identifiers is also not regarded as processing of sensitive data in the meaning of Art. 8 (1).

3. Member States

3.1. Implementation of Art. 8 Directive 95/46/EC

Art. 8 of Directive 95/46/EC concerning the processing of sensitive data has been implemented in all Member States in largely similar fashion. There are differences, however, concerning the respective categories of sensitive data referred to in Art. 8 (1) and the grounds for exceptions under Art. 8 (2) through (4) and (5).

3.1.1. Data categories, Art. 8 (1) Directive 95/46/EC

All the data protection laws of the Member States include the same catalogue of data types found in Art. 8 (1) of the Directive.

Some Member States have added genetic data and biometric data; one Member State regards "private life" as sensitive data, other Member States "party membership" (in addition to trade-union membership) and "addictions".

Further, a few Member States have also included data from the judiciary in their catalogue of special categories of personal data, for example information about previous convictions or criminal behaviour. This represents a derogation from Art. 8 (5) of the Directive, in which such data are not considered sensitive in the meaning of Art. 8 (1) of the Directive.

Beyond sensitive data, one Member State considers specific categories of treatments as "risky". Such "risky" treatments include for instance genetic data, biometric data and information about criminal records. Processing such data is not prohibited as such but is subject to prior authorisation from the data protection supervisory authority.

3.1.2. Exceptions, Art. 8 (2) – (4), (5), (7) Directive 95/46/EC

The exceptions under Art. 8 (2) – (4), (5) and (7) of Directive 95/46/EC allowing the processing of sensitive data, data relating to offences and national identification numbers, have also been implemented in mostly uniform fashion in the Member States. Differences and a strong tendency towards sector-specific rules are noticeable in particular where the Directive makes only general provisions for exceptions and the Member States thus have a great deal of discretion.

This applies especially to Art. 8 (4) of the Directive stating that Member States may, "for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2" of Art. 8. The Member States have made extensive use of this power and created a variety of special legal exceptions for the processing of sensitive data.

These include for example data processing for the purpose of protecting public security, ensuring the ability of government bodies and authorities to function, preventing serious detriment to the common good, fighting crime, providing equal opportunity as well as social protection and pension systems; for the purpose of scientific research and statistics and for journalistic or artistic purposes. In addition, exceptions cover the areas of preventive medicine, social protection, banking, taxes and customs, labour market policy and unemployment insurance, foreigners and administrative enforcement. One Member State ruled that special data may be processed, if it is "ordered by an Act", thus creating potentially wide exceptions.

A few Member States also have special exceptions for the processing of genetic data, although such processing either requires prior permission by the data protection supervisory authority or is only permitted for narrowly defined purposes, such as criminal investigations, protection of vital interests or on important medical grounds.

There are also differences in the implementation of Art. 8 (5) of the Directive which allows the processing of data related to criminal offences, "if suitable specific safeguards are provided under national law". In this context, the Member States have either defined the relevant data as an additional category of sensitive data or have created a special legal framework including certain conditions for processing such data.

In addition, a few Member States have taken advantage of the possibility under Art. 8 (7) of the Directive to determine the conditions under which a national identification number may be processed.

3.2. Problems of application

3.2.1. Data categories, Art. 8 (1) Directive 95/46/EC

The data protection authorities see the following problems, among others, in applying the concept of sensitive data in the Member States:

- It is difficult to define "philosophical beliefs" as referred to in Art. 8 (1) of the Directive. For example, a court in the U.K. recognized belief in climate change as a philosophical belief.

- Photos and images of persons, such as those published on the Internet or taken by traffic monitoring or other surveillance cameras, are especially problematic. Since images can reveal information about an individual's ethnic origin or health status, for example, they may be considered sensitive data as defined in Art. 8 (1) of the Directive, with the result that these data may not be processed without the individual's consent.

- Other categories of data display major differences in the degree of sensitivity. For example, health data may range from information about a simple cold to stigmatizing information about illnesses or disabilities. This leads to difficulties in practice, as the individual's consent is required even for unproblematic processing of such data.

- There are differences in applying certain categories of sensitive data in Member States, because the degree of sensitivity may be seen in one Member State differently than in another Member State, e.g. with regard to the category "trade-union membership".

3.2.2. Exceptions, Art. 8 (2) – (4), (5), (7) Directive 95/46/EC

As a result of the prohibition of processing sensitive data according to Art. 8 (1) of the Directive, such data may be processed only when the data subject has given explicit consent or when one of the exceptions mentioned in Art. 8 (2) – (4), (5) and (7) applies. In this context the following difficulties were reported:

- Art. 8 (3) of the Directive, which states that sensitive data may be processed only by health professionals or other persons obliged to an equivalent secrecy obligation, may lead to difficulties in the health-care sector, because in practice health data are processed for various purposes and it is often not clear who belongs to the category of health professionals or the group of persons obliged to comparable secrecy obligations. Nor are there currently explicit grounds under Art. 8 of the Directive justifying the processing of

sensitive personal data in case of injuries, when health data are transmitted by non-medical personnel, e.g. at schools.

- As regards the insurance sector, the processing of health data is a necessary prerequisite for concluding and performing a health insurance contract. Art. 8 (3) of the Directive, however, does not explicitly allow the usage of health data for insurance purposes. In the absence of a respective exception, data subjects are regularly faced with signing complicated declarations of consent, which often do not meet the legal requirements of informed consent. In practice, insurance companies, for example, use blanket declarations which cover numerous forms of data processing. It is doubtful whether insurants in these cases generally have a clear understanding of what they are consenting and it is furthermore questionable if the "consent" in these cases is free.

- A similar situation exists with respect to the processing of data which are subject to professional secrecy, for example, the processing of sensitive personal data by lawyers or tax advisers, in particular, if those data is transferred to third parties or is processed by a processor.

- Where, according to national law, explicit consent is a prerequisite for the processing of sensitive data, problems may occur when consent is required in an electronic environment. In those circumstances, written consent may only be given by using secure electronic signatures, which, however, are rarely used by citizens in practice.

- Another problem in applying Art. 8 of the Directive has been reported by the European Commission: According to Art. 8 (6) of the Directive derogations from Art. 8 (1) on the basis of Art. 8 (4) and (5) shall be notified to the Commission. In practice this obligation is not always met by Member States. Thus, for the Commission it is difficult to provide an EU-wide overview of those derogations from Art. 8 (1). This is problematic in particular with regard to Art. 8 (4) as this provision – as has been shown (above 3.1.2.) – is used by Member States for a broad range of exceptions allowing for the processing of sensitive data for different purposes.

III. Need for revision seen by the Article 29 Working Party

Most members of the Working Party see a need for revising Art. 8 of Directive 95/46/EC, although they differ on the substance and on the extent of the revision.

Some members favour revising the basic approach to sensitive data in order to increase flexibility and take account of the processing context, while other members see less or no need to change the basic concept but consider it advisable to expand the catalogue of sensitive data and/or exceptions.

1. Revision of data categories and possible additional safeguards

1.1. Current categories of sensitive data

- **Racial or ethnic origin**

The Working Party finds the term "race" unclear. According to recent scientific thought, there are no races. In biological terms, Homo sapiens today is not divided into different races nor sub-types. Since the 1970s, molecular biology and population genetics have shown that such systematic divisions fail to do justice to the tremendous diversity of and fluid transitions between geographic populations. Further, most genetic differences between people are found within a single geographic population. Dividing humans into different races thus no longer reflects the state of current scientific research. What is meant here is only protection of certain data due to their reference to a particular ethnic group. For this reason, the words "racial or" should be replaced.

- **Political opinions, religious or philosophical beliefs**

The Working Party finds the term "philosophical beliefs" difficult to define for practical purposes. A more precise term would be preferable.

- **Health-related data**

The Working Party finds that, due to the wide range of personal data that may fall into the category of health-related data, this category represents one of the most complex areas of sensitive data and one where the Member States display a great deal of legal uncertainty. Special measures are needed to protect health data, the processing of which is associated with serious privacy infringements, against abuse (e.g. the commercial use of patient data). A particular problem relates to the processing of health data for insurance purposes (see 3.2.2. above).

1.2. Proposed new categories of sensitive data

With regard to the data categories listed in Art. 8 (1) of the Directive, the majority of Working Party members are in favour of explicitly including genetic data in the catalogue of sensitive data. Some DPAs are also in favour of including biometric data and the creation of personal profiles. Some DPAs also proposed as additional categories data of minors, information about individuals' financial situation and data on an individuals´ geo-location, in particular when the latter is processed in the context of electronic networks. Several Member States also believe that the context and/or the purpose of processing should be taken into account when assessing the issue of sensitivity.

In the view of the Working Party, genetic and biometric data, as well as possible further new categories of sensitive data, should not be enacted without the support of a solid definition.

1.3. Additional safeguards

The Directive in its current approach does not contain any specific rules on the security of processing sensitive personal data which would go beyond the general requirements on data security in Art. 17 of the Directive. Currently it may therefore appear that sensitive data are in practice no more protected than data that do not fall under this category. Given that sensitive data should be specially protected due to their nature and possible harm to the individual, in the Working Party's view additional legal, organisational and technical safeguards should be considered. The Working Party recommends an approach that builds upon existing and well-accepted international standards in the field of information security. Organisational and technical safeguards could for example include measures such as the introduction of Information Security Managements Systems (e.g. ISO/IEC standards) based on the analysis of information resources and underlying threats, measures for cryptographic protection during storage and transfer of sensitive data, requirements for authentication and authorisation, physical and logical access to data, access logging and others. Additional legal safeguards could reinforce information rights of data subjects, accentuate strict relevance of processing or introduce other specific safeguards.

Moreover, persons involved in the processing of sensitive personal data could be obliged to respective secrecy obligations, e.g. as part of employment contracts.

2. Exceptions, Art. 8 (2) – (4), (5), (7) Directive 95/46/EC

Given the diversity of implementation at national level, the Working Party finds that revising the exceptions in Art. 8 (2) – (4), (5), (7) of the Directive should be considered.

- The Working Party sees a need for revision in Art. 8 (3) on the processing of health data. In the Member States, problems have arisen in data protection practice with regard to the broad range of health data and the term "health professional", in addition, specific problems in the processing of health data for insurance purposes have occurred (see above II. 3.2.1. and 3.2.2.).

- The Working Party also sees a need to formulate more precisely the exception for the processing of sensitive data "for reasons of substantial public interest" (Art. 8 (4)). The Working Party recommends taking Art. 52 (1) of the EU Charter of Fundamental Rights as a model and allowing processing only if provided for by a legal act which clearly sets out the purposes and grounds (which must reflect a substantial public interest) for the processing of sensitive personal data. Such processing must also be possible to protect vital interests of the data subject or other persons.

- The Working Party also calls for defining the term "safeguards" in Art. 8 (2), (4), (5) (also used elsewhere in the Directive as a whole) more precisely and possibly by giving examples, for instance with regard to data security requirements which must be observed when processing sensitive data (beyond Art. 17 Directive 95/46/EC, see above 1.3) or subject to specific notification and permit requirements.

- Given that the former 3rd Pillar is to be included in the future legal framework, the Working Party believes it may be necessary to revise the catalogue of exemptions, for example, by mentioning in Art. 8 (5) the processing by police and justice authorities and

of Member State courts of personal data related to criminal offences. The term "suitable safeguards" used in (5) should be more precisely defined in this context as well. The Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters should be taken into account in order to build a coherent legal framework on data protection in the EU.

3. Analysis of alternative approaches

In the view of existing problems of application of Art. 8 (see above II.3.2.) and the partially significant lack of harmonisation in the implementation of Art. 8 para. (2) – (4) and (5), the Working Party discussed whether or not a change in the basic approach to the processing of sensitive data should be considered. The following options were put forward:

Option 1 (current approach):

Maintain the current concept of a general prohibition of processing of sensitive data and a closed list of data categories, with possible amendments to the data categories and/or exceptions.

Option 2 (context approach):

General prohibition of a list of data categories (current + possible additional) which by their nature should be regarded as sensitive, but leave discretion for Member States to decide upon further categories (approach corresponds to Art. 6, 11 Council Convention 108 and Section 13 of the Madrid Resolution on International Standards). Include a general definition of sensitive data which also takes the processing context into account.[5]

Option 3 (precautionary principle):

Precautionary Principle (on basis of Council of Europe Convention 108): Change the perspective, on the basis of the "precautionary principle": sensitive data may not be processed "unless" domestic law provides appropriate safeguards.

In addition, it had been suggested to supplement option 1 above by a revision mechanism, whereby the list of special categories should be regularly revised. If a revision mechanism would be subject to the comitology-procedure, consequently the list of categories of sensitive data needs to be put in an Annex to the Directive.

In the Working Party's advice paper, the aforementioned alternatives could have the following possible impacts both in legal and in practical terms:

[5] According to this view, a possible wording for a revised Art. 8 (1) could be as follows: "Member States shall prohibit the processing of sensitive personal data. Sensitive personal data are personal data, which are capable by their nature or by the context in which they are processed of infringing fundamental freedoms or privacy or which have an especially discriminatory effect on the data subject. Personal data, which by their nature are regarded as sensitive are personal data revealing ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concern health or sex life. Member States may lay down other categories of sensitive data where the conditions referred to in this paragraph are met."

3.1. Option 1 (current approach)

This approach builds on the premise that the current approach has proven to be generally successful. Possible amendments refer to the list of data categories (add new categories), the exemptions (more harmonization) and possible additional safeguards for processing (beyond Art. 17).

The following main advantages of the current approach have been identified:

- A strong political signal, that the processing of sensitive data is generally prohibited;

- a high degree of harmonization as regards the categories of sensitive data in the meaning of Art. 8 (1);

- legal certainty for data controllers as regards the application of these categories.

The main disadvantages of the current approach are:

- A closed list is inflexible and unable to react to the context of processing as well as new forms of processing which might occur in the course of ongoing technological developments;

- a closed list does not take legal and cultural differences in Member States into account;

- harmonization has been achieved regarding the data categories in the meaning of Art. 8 (1), but not in the field of the exceptions in (2) – (5), where significant differences exist in national implementing legislation.

3.2. Option 2 (context approach)

The Working Party also discussed whether the current approach to sensitive data should be more flexible and should also take the context of processing into account.

The following main advantages of the context approach have been identified:

- Strong political signal, that the processing of certain categories of personal data, which are regarded as sensitive by their nature (current list + possible additional categories) is generally prohibited;

- discretion for Member States to decide upon further categories (same approach as Council Convention 108 and the Madrid resolution on International Standards), thus leaving space to react to new forms of sensitive data; accepting cultural/legal differences;

- includes the context of processing and provides protection against possible new forms of processing methods which might occur in the light of ongoing technological developments.

The main disadvantages of a context approach are:

- Differences in national legislation regarding possible further categories of sensitive data;

- legal uncertainty for data controllers as regards possible further categories;

- in the field of exceptions, great differences between national legislation exist (alike current approach, 3.1.).

3.3. Option 3 (precautionary principle)

According to other views represented in the Working Party, future EU legal provisions on sensitive data could be more closely oriented on Art. 6 of the Council of Europe's Data Protection Convention, which does not prohibit the processing of sensitive data in general, but rather makes the processing of such data conditional on whether domestic law provides appropriate safeguards (see II.1 above on Art. 6 of Convention No. 108).

In the Working Party's view, the basic approach of Art. 6 Convention 108 in essence does not differ significantly from the approach taken by the Directive as it does not make a difference whether the processing of sensitive data is permitted only under certain safeguards (Convention approach) or only under certain exceptions (Directive approach). In both cases, an unconditional processing of sensitive data is basically forbidden, even if the Convention – different than Art. 8 (1) – does not explicitly provide for the prohibition of processing.

However, this perspective leaves in principle more margin of manoeuvre to Member States than the Directive to allow for the processing of sensitive data. If this approach is followed, measures should nevertheless be taken to ensure enough legal certainty: there must be sufficient harmonisation between Member States with regard to the conditions according to which sensitive data can be processed. The conditions and safeguards could at the end be very similar in substance to those foreseen in options 1. and 2.

A difference, however, lies in the fact, that the Convention is more flexible since it leaves the parties discretion to define further categories of data not explicitly mentioned in Art. 6 as "sensitive", thereby accepting the possibility of differences between national regulatory regimes. This would mean less harmonization between Member States in what should be regarded as sensitive data. On the other hand, this discretion would lead to greater flexibility as regards possible new issues of sensitivity, which might occur in practice in Member States. Since the Convention does not define which "safeguards" should be a prerequisite for the processing of sensitive data, it also leaves a significant degree of discretion to the parties to the Convention also in this respect. If this option is preferred for the future EU framework, harmonisation should still be ensured with regard to the details of the safeguards implemented at national level, in order to provide sufficient legal certainty to data subjects and controllers over the EU.

The following advantages of the precautionary principle have been identified:

- Political signal that the unconditional processing of sensitive data is prohibited;

- harmonization as regards the current list of categories;

- discretion for Member States to decide upon further categories, thus leaving space to react to new forms of sensitive data; accepting cultural/legal differences.

The main disadvantages are:

- Differences in national legislation regarding possible further categories of sensitive data;

- term and scope of concept “safeguards” unclear;

- legal uncertainty regarding conditions (exemptions/safeguards), under which sensitive data might be processed.

IV. Conclusions

The Data Protection Directive 95/46/EC and the Council of Europe Data Protection Convention of 1981 are based on the premise that certain categories of personal data, as distinct from all other personal data, require extra protection and may therefore be processed by private and public bodies only for specific purposes and under special conditions.

In this advice paper the Working Party analyses in greater detail the rationale and the scope of the current concept of “special categories of data” (“sensitive data”) on EU and Member State’s level, examines possible improvements of the existing approach and analyses different alternatives to the current system.

Against the background of the discussions of the Working Party on this complex issue, the following conclusions can be drawn:

Data Categories:

- Basically Art. 8 (1) has been implemented in a harmonized fashion; the current category “race” appears to be problematic, the terms “philosophical beliefs” and “health data” appear to be too broad (III.1.1.). Regarding new categories, the majority of the Working Party supports including genetic data and biometric data. All data categories should be legally defined.

Exceptions:

- As a result of the usage of unspecified legal terms in the current Directive like “public interest” in (4), “health data” in (3), “safeguards” in (2), (4), (5) and the broad range of exceptions for processing of sensitive data under Art. 8 (2) – (5) as such, Member States have used their discretion in a different fashion with the result of significant differences in the implementation of Art. 8 (2) – (5). (see II.3.1.2.). Unspecified legal terms should, therefore, to the greatest possible extent be avoided or legally defined.

- Specific problems in practice have occurred in the context of processing of health data (II.3.2.2.).

- Exceptions for processing of sensitive data should – in line with Art. 52 (1) of the EU Charter of Fundamental Rights – be explicitly allowed only if provided for by a legal act which clearly sets out the purposes and grounds for the processing of sensitive personal data. Such processing must also be possible to protect vital interests of the data subject or other persons.

Additional safeguards:

- Specific provisions on data security (technical and organisational) for the processing of sensitive data required which go beyond Art. 17 (see III.1.3.), as well additional legal safeguards.

Basic approach:

- Several members of the WP favour the existing system (closed list, general prohibition of processing of sensitive data with exemptions), however, supports changes to the data categories and/or the exemptions as outlines above (III.3. and 3.1.). In addition it has been suggested to introduce a revision mechanism for current and possible new categories of sensitive data. If this revision should be subject to the comitology procedure, the list of sensitive data needs to be put in an Annex to the Directive (III.3.).

- Other members of the WP support a context-approach: General prohibition of a list of data categories (current + possible additional) which by their nature should be regarded as sensitive, but leave discretion for Member States to decide upon further categories (approach corresponds to Art. 6, 11 Council Convention 108 and Section 13 of the Madrid Resolution on International Standards). Include a general definition of sensitive data which also takes the processing context into account (III.3. and 3.2.; for a possible wording of a revised Art. 8 (1) of Directive 95/46/EC see above III.3, footnote no. 5).

- Precautionary Principle (on basis of Council of Europe Convention 108): Processing of sensitive data only allowed under specific safeguards. Discretion for Member States to decide upon further data categories (III.3 and 3.3.).

Done at Brussels, on 4 April 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM