

Project acronym: **ASSET**
Project full title: Aeronautic Study on Seamless Transport
Grant agreement no.: **FP7 - 211625**
SEVENTH FRAMEWORK PROGRAM
Transport
Aeronautics and Air Transport

WP: WP1
Deliverable No.: Annex to D1.2
Originator: ID PARTNERS

ANNEX to: Report on privacy constraints and the work carried on by standardization bodies



Due date of deliverable:	Actual submission date:
Start date of project: 01/06/2008	Duration: 36 months
Project coordinator: DLR	Revision:

Change Records

Version	Date	Changes	Author
			ID PARTNERS

1	ANNEXES	4
1.1	Commission Regulation (EU) No 18/2010	5
1.2	COM(2005) 429 final	20
1.3	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	30
1.4	COMMON STANDARDS FOR SAFEGUARDING CIVIL AVIATION	46
1.5	Directive 95/46/EC	53
1.6	Directive 97/66	91
1.7	Directive 2002/58	106
1.8	PETs Privacy Enhancing Technologies	131
1.9	Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the processing of Personal Data.	141
1.10	Passenger Information Unit	151

1 ANNEXES

We have included as ANNEX the main regulatory documents addressing aviation security and passengers' privacy

1.1 Commission Regulation (EU) No 18/2010

Amendment of Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programs in the field of civil aviation security are concerned

Official Journal L 007 , 12/01/2010 P. 0003 - 0014

Published : 8 January 2010

THE EUROPEAN COMMISSION,

Having regard to the Treaty on European Union and to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 [1], and in particular Article 11(2) thereof,

Whereas:

(1) The development and implementation of a national quality control program by each Member State is essential to ensure the effectiveness of its national civil aviation security program in accordance with Article 11(1) of Regulation (EC) No 300/2008.

(2) Specifications for the national quality control program to be implemented by the Member States should ensure a harmonised approach in this respect.

(3) To be effective, compliance monitoring activities to be undertaken under the responsibility of the appropriate authority should be carried out regularly. They should not be restricted as to the subject, stage or moment at which they are carried out. They should take the most suitable forms to ensure their effectiveness.

(4) Priority should be given to the development of a common methodology for compliance monitoring activities.

(5) It is necessary to develop a harmonised way of reporting on the measures taken to fulfil the obligations under this Regulation and on the aviation security situation in the territories of the Member States.

(6) National quality control programs should be based on best practices. Such best practices should be shared with the Commission and communicated to all Member States.

(7) Regulation (EC) No 300/2008 should therefore be amended accordingly.

(8) The measures provided for in this Regulation are in accordance with the opinion of the Committee for Civil Aviation Security,

HAS ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EC) No 300/2008

Regulation (EC) No 300/2008 is amended as follows:

1. The title "Annex" is replaced by "Annex I".
2. The text set out in the Annex to this Regulation is added as Annex II.

Article 2

Entry into force

This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union.

It shall apply as from the date specified in the implementing rules adopted in accordance with the procedure referred to in Article 4(3) of Regulation (EC) No 300/2008, but not later than 29 April 2010.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 January 2010.

For the Commission

The President

José Manuel Barroso

[1] OJ L 97, 9.4.2008, p. 72.

ANNEX II

Common specifications for the national quality control program to be implemented by each Member State in the field of civil aviation security

1. DEFINITIONS

1.1. For the purposes of this Annex, the following definitions shall apply:

(1) "annual traffic volume" means the total number of passengers arriving, departing and in transit (counted once);

(2) "appropriate authority" means the national authority designated by a Member State pursuant to Article 9 to be responsible for the coordination and monitoring of the implementation of its national civil aviation security program;

(3) "auditor" means any person conducting national compliance monitoring activities on behalf of the appropriate authority;

(4) "certification" means a formal evaluation and confirmation by or on behalf of the appropriate authority that a person possesses the necessary competencies to perform the functions of an auditor to an acceptable level as defined by the appropriate authority;

(5) "compliance monitoring activities" means any procedure or process used for assessing the implementation of this Regulation and the national aviation security program;

(6) "deficiency" means a failure to comply with an aviation security requirement;

(7) "inspection" means an examination of the implementation of security measures and procedures in order to determine whether they are being carried out effectively and to the required standard and to identify any deficiencies;

(8) "interview" means an oral check by an auditor to establish whether specific security measures or procedures are implemented;

(9) "observation" means a visual check by an auditor that a security measure or procedure is implemented;

(10) "representative sample" means a selection made from amongst possible options for monitoring which is sufficient in number and range to provide a basis for general conclusions on implementing standards;

(11) "security audit" means an in-depth examination of security measures and procedures in order to determine if they are being fully implemented on a continual basis;

(12) "test" means a trial of aviation security measures, where the appropriate authority simulates intent to commit an act of unlawful interference for the purpose of examining the effectiveness of the implementation of existing security measures;

(13) "verification" means an action taken by an auditor to establish whether a specific security measure is actually in place;

(14) "vulnerability" means any weakness in the implemented measures and procedures which could be exploited to carry out an act of unlawful interference.

2. POWERS OF THE APPROPRIATE AUTHORITY

2.1. Member States shall provide the appropriate authority with the necessary powers for monitoring and enforcing all requirements of this Regulation and its implementing acts, including the power to impose penalties in accordance with Article 21.

2.2. The appropriate authority shall perform compliance monitoring activities and have the powers necessary to require any identified deficiency to be rectified within set timeframes.

2.3. A graduated and proportionate approach shall be established regarding deficiency correction activities and enforcement measures. This approach shall consist of progressive steps to be followed until correction is achieved, including:

- (a) advice and recommendations;
- (b) formal warning;
- (c) enforcement notice;
- (d) administrative sanctions and legal proceedings.

The appropriate authority may omit one or more of these steps, especially where the deficiency is serious or recurring.

3. OBJECTIVES AND CONTENT OF THE NATIONAL QUALITY CONTROL PROGRAM

3.1. The objectives of the national quality control program are to verify that aviation security measures are effectively and properly implemented and to determine the level of compliance with the provisions of this Regulation and the national civil aviation security program, by means of compliance monitoring activities.

3.2. The national quality control program shall include the following elements:

- (a) organisational structure, responsibilities and resources;
- (b) job descriptions of, and qualifications required for auditors;
- (c) compliance monitoring activities, including scope of security audits, inspections, tests and, following an actual or potential breach of security, investigations, frequencies for security audits and inspections and also classification of compliance;
- (d) surveys, where there is cause to reassess security needs;
- (e) deficiency correction activities providing details concerning deficiency reporting, follow-up and correction in order to ensure compliance with aviation security requirements;

(f) enforcement measures and, where appropriate, penalties, as specified in points 2.1 and 2.3 of this Annex;

(g) reporting of compliance monitoring activities carried out including, where appropriate, information exchange between national bodies on compliance levels;

(h) monitoring process of the airport, operator and entity internal quality control measures;

(i) a process to record and analyse the results of the national quality control program to identify trends and steer future policy development.

4. COMPLIANCE MONITORING

4.1. All airports, operators and other entities with aviation security responsibilities shall be regularly monitored to ensure the swift detection and correction of failures.

4.2. Monitoring shall be undertaken in accordance with the national quality control program, taking into consideration the threat level, type and nature of the operations, standard of implementation, results of internal quality control of airports, operators and entities and other factors and assessments which will affect the frequency of monitoring.

4.3. Monitoring shall include the implementation and effectiveness of the internal quality control measures of airports, operators and other entities.

4.4. Monitoring at each individual airport shall be made up of a suitable mixture of compliance monitoring activities and provide a comprehensive overview of the implementation of security measures in the field.

4.5. The management, setting of priorities and organisation of the quality control program shall be undertaken independently from the operational implementation of the measures taken under the national civil aviation security program.

4.6. Compliance monitoring activities shall include security audits, inspections and tests.

5. METHODOLOGY

5.1. The methodology for conducting monitoring activities shall conform to a standardised approach, which includes tasking, planning, preparation, on-site activity, the classification of findings, the completion of the report and the correction process.

5.2. Compliance monitoring activities shall be based on the systematic gathering of information by means of observations, interviews, examination of documents and verifications.

5.3. Compliance monitoring shall include both announced and unannounced activities.

6. SECURITY AUDITS

6.1. A security audit shall cover:

- (a) all security measures at an airport; or
- (b) all security measures implemented by an individual airport, terminal of an airport, operator or entity; or
- (c) a particular part of the National Civil Aviation Security Program.

6.2. The methodology for conducting a security audit shall take into consideration the following elements:

- (a) announcement of the security audit and communication of a pre-audit questionnaire, if appropriate;
- (b) preparation phase including examination of the completed pre-audit questionnaire and other relevant documentation;
- (c) entry briefing with airport/operator/entity representatives prior to beginning the monitoring activity on-site;
- (d) on-site activity;
- (e) debriefing and reporting;
- (f) where deficiencies are identified, the correction process and the associated monitoring of that process.

6.3. In order to confirm that security measures are implemented, the conduct of a security audit shall be based on a systematic gathering of information by one or more of the following techniques:

- (a) examination of documents;
- (b) observations;
- (c) interviews;
- (d) verifications.

6.4. Airports with an annual traffic volume of more than 10 million passengers shall be subject to a security audit covering all aviation security standards at least every 4 years. The examination shall include a representative sample of information.

7. INSPECTIONS

7.1. The scope of an inspection shall cover at least one set of directly linked security measures of Annex I to this Regulation and the corresponding implementing acts monitored as a single activity or within a reasonable time frame, not normally exceeding three months. The examination shall include a representative sample of information.

7.2. A set of directly linked security measures is a set of two or more requirements as referred to in Annex I to this Regulation and the corresponding implementing acts which impact on each other so closely that achievement of the objective cannot be adequately assessed unless they are considered together. These sets shall include those listed in Appendix I to this Annex.

7.3. Inspections shall be unannounced. Where the appropriate authority considers that this is not practicable, inspections may be announced. The methodology for conducting an inspection shall take into consideration the following elements:

- (a) preparation phase;
- (b) on-site activity;
- (c) a debrief, depending on the frequency and the results of the monitoring activities;
- (d) reporting/recording;
- (e) correction process and its monitoring.

7.4. In order to confirm that security measures are effective, the conduct of the inspection shall be based on the systematic gathering of information by one or more of the following techniques:

- (a) examination of documents;
- (b) observations;
- (c) interviews;
- (d) verifications.

7.5. At airports with an annual traffic volume of more than 2 million passengers the minimum frequency for inspecting all sets of directly linked security measures set out in chapters 1 to 6 of Annex I to this Regulation shall be at least every 12 months, unless an audit has been carried out at the airport during that time. The frequency for inspecting all security measures covered by chapters 7 to 12 of Annex I shall be determined by the appropriate authority based on a risk assessment.

7.6. Where a Member State has no airport with an annual traffic volume exceeding 2 million passengers, the requirements of point 7.5 shall apply to the airport on its territory with the greatest annual traffic volume.

8. TESTS

8.1. Tests shall be carried out to examine the effectiveness of the implementation of at least the following security measures:

- (a) access control to security restricted areas;
- (b) aircraft protection;
- (c) screening of passengers and cabin baggage;
- (d) screening of staff and items carried;
- (e) protection of hold baggage;
- (f) screening of cargo or mail;
- (g) protection of cargo and mail.

8.2. A test protocol including the methodology shall be developed taking into consideration the legal, safety and operational requirements. The methodology shall address the following elements:

- (a) preparation phase;
- (b) on-site activity;
- (c) a debrief, depending on the frequency and the results of the monitoring activities;
- (d) reporting/recording;
- (e) correction process and the associated monitoring.

9. SURVEYS

9.1. Surveys shall be carried out whenever the appropriate authority recognises a need to re-evaluate operations in order to identify and address any vulnerabilities. Where a vulnerability is identified, the appropriate authority shall require the implementation of protective measures commensurate with the threat.

10. REPORTING

10.1. Compliance monitoring activities shall be reported or recorded in a standardised format which allows for an on-going analysis of trends.

10.2. The following elements shall be included:

(a) type of activity;

(b) airport, operator or entity monitored;

(c) date and time of the activity;

(d) name of the auditors conducting the activity;

(e) scope of the activity;

(f) findings with the corresponding provisions of the National Civil Aviation Security Program;

(g) classification of compliance;

(h) recommendations for remedial actions, where appropriate;

(i) time frame for correction, where appropriate.

10.3. Where deficiencies are identified, the appropriate authority shall report the relevant findings to the airport, operators or entities subjected to monitoring.

11. COMMON CLASSIFICATION OF COMPLIANCE

11.1. Compliance monitoring activities shall assess the implementation of the national civil aviation security program using the harmonised classification system of compliance set out in Appendix II.

12. CORRECTION OF DEFICIENCIES

12.1. The correction of identified deficiencies shall be implemented promptly. Where the correction cannot take place promptly, compensatory measures shall be implemented.

12.2. The appropriate authority shall require airports, operators or entities subjected to compliance monitoring activities to submit for agreement an action plan addressing any deficiencies outlined in the reports together with a timeframe for implementation of the remedial actions and to provide confirmation when the correction process has been completed.

13. FOLLOW-UP ACTIVITIES RELATED TO THE VERIFICATION OF THE CORRECTION

13.1. Following confirmation by the airport, operator or entity subjected to monitoring that any required remedial actions have been taken, the appropriate authority shall verify the implementation of the remedial actions.

13.2. Follow-up activities shall use the most relevant monitoring method.

14. AVAILABILITY OF AUDITORS

14.1. Each Member State shall ensure that a sufficient number of auditors are available to the appropriate authority directly or under its supervision for performing all compliance monitoring activities.

15. QUALIFICATION CRITERIA FOR AUDITORS

15.1. Each Member State shall ensure that auditors performing functions on behalf of the appropriate authority:

(a) are free from any contractual or pecuniary obligation to the airport, operator or entity to be monitored; and

(b) have the appropriate competencies, which include sufficient theoretical and practical experience in the relevant field.

Auditors shall be subject to certification or equivalent approval by the appropriate authority.

15.2. The auditors shall have the following competencies:

(a) an understanding of current applicable security measures and how they are applied to the operations being examined including:

- an understanding of security principles,
- an understanding of supervisory tasks,
- an understanding of factors affecting human performance,

(b) a working knowledge of security technologies and techniques;

(c) a knowledge of compliance monitoring principles, procedures and techniques;

(d) a working knowledge of the operations being examined;

(e) an understanding of the role and powers of the auditor.

15.3. Auditors shall undergo recurrent training at a frequency sufficient to ensure that existing competencies are maintained and new competencies are acquired to take account of developments in the field of security.

16. POWERS OF AUDITORS

16.1. Auditors carrying out monitoring activities shall be provided with sufficient authority to obtain the information necessary to carry out their tasks.

16.2. Auditors shall carry a proof of identity authorising compliance monitoring activities on behalf of the appropriate authority and allowing access to all areas required.

16.3. Auditors shall be entitled to:

(a) obtain immediate access to all relevant areas including aircraft and buildings for monitoring purposes; and

(b) require the correct implementation or repetition of the security measures.

16.4. As a consequence of the powers conferred on auditors, the appropriate authority shall act in accordance with point 2.3 in the following cases:

(a) intentional obstruction or impediment of an auditor;

(b) failure or refusal to supply information requested by an auditor;

(c) when false or misleading information is supplied to an auditor with intent to deceive; and

(d) impersonation of an auditor with intent to deceive.

17. BEST PRACTICES

17.1. Member States shall inform the Commission of best practices with regard to quality control programs, audit methodologies and auditors. The Commission shall share this information with the Member States.

18. REPORTING TO THE COMMISSION

18.1. Member States shall annually submit a report to the Commission on the measures taken to fulfil their obligations under this Regulation and on the aviation security situation at the airports located in their territory. The reference period for the report shall be 1 January – 31 December. The report shall be due three months after completion of the reference period.

18.2. The content of the report shall be in accordance with Appendix III using a template provided by the Commission.

18.3. The Commission shall share the main conclusions drawn from these reports with Member States.

Appendix I

Elements to be included in the set of directly linked security measures

The sets of directly linked security measures as referred to in point 7.1 of Annex II shall include the following elements of Annex I to this Regulation and the corresponding provisions in its implementing acts:

For point 1 — Airport security:

- (i) point 1.1; or
- (ii) point 1.2 (except provisions relating to identification cards and vehicle passes); or
- (iii) point 1.2 (provisions relating to identification cards); or
- (iv) point 1.2 (provisions relating to vehicle passes); or
- (v) point 1.3 and the relevant elements of point 12; or
- (vi) point 1.4; or
- (vii) point 1.5.

For point 2 — Demarcated areas of airports:

the whole point

For point 3 — Aircraft security:

- (i) point 3.1; or
- (ii) point 3.2.

For point 4 — Passengers and cabin baggage:

- (i) point 4.1 and the relevant elements of point 12; or
- (ii) point 4.2; or
- (iii) point 4.3.

For point 5 — Hold baggage:

- (i) point 5.1 and the relevant elements of point 12; or
- (ii) point 5.2; or

(iii) point 5.3.

For point 6 — Cargo and mail:

(i) all provisions relating to screening and security controls applied by a regulated agent, except as detailed in points (ii) to (v) below; or

(ii) all provisions relating to security controls applied by known consignors; or

(iii) all provisions relating to account consignors; or

(iv) all provisions relating to the transportation of cargo and mail; or

(v) all provisions relating to the protection of cargo and mail at airports.

For point 7 — Air carrier mail and air carrier materials:

the whole point

For point 8 — In-flight supplies:

the whole point

For point 9 — Airport supplies:

the whole point

For point 10 — In-flight security measures:

the whole point

For point 11— Staff recruitment and training:

(i) all provisions relating to staff recruitment at airport, air carrier or entity; or

(ii) all provisions relating to staff training at an airport, air carrier or entity.

Appendix II

Harmonised classification system of compliance

The following classification of compliance shall apply to assess the implementation of the national civil aviation security program.

Appendix III

CONTENT OF REPORT TO THE COMMISSION

1. Organisational structure, responsibilities and resources

(a) Structure of the quality control organisation, responsibilities and resources, including planned future amendments (see point 3.2(a)).

(b) Number of auditors – present and planned (see point 14).

(c) Training completed by auditors (see point 15.2).

2. Operational monitoring activities

All monitoring activities carried out, specifying:

(a) type (security audit, initial inspection, follow up inspection, test, other);

(b) airports, operators and entities monitored;

(c) scope;

(d) frequency; and

(e) total man-days spent in the field.

3. Deficiency correction activities

(a) Status of the implementation of the deficiency correction activities.

(b) Main activities undertaken or planned (e.g. new posts created, equipment purchased, construction work) and progress achieved towards correction.

(c) Enforcement measures used (see point 3.2(f)).

4. General data and trends

(a) Total national annual passenger and freight traffic and number of aircraft movements.

(b) List of airports by category.

(c) Number of air carriers operating from the territory by category (national, EU, third country).

(d) Number of regulated agents.

(e) Number of catering companies.

(f) Number of cleaning companies.

(g) Approximate number of other entities with aviation security responsibilities (known consignors, ground handling companies).

5. Aviation security situation at airports

General context of the aviation security situation in the Member State.

1.2 COM(2005) 429 final

Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security /* COM/2005/0429 final - COD 2005/0191 */

COMMISSION OF THE EUROPEAN COMMUNITIES |

Brussels, 22.9.2005

2005/0191 (COD)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- Grounds for and objectives of the proposal

Regulation (EC) No 2320/2002 of the European Parliament and of the Council establishing common rules in the field of civil aviation security has been in force since January 2003. Experience gained on the basis of Commission inspections and the daily application of the Regulation by Member States shows that the swift transformation into legislation of a set of non-binding recommendations developed by the Member States has led, due to the quick drafting and adoption of the Regulation as a response to the events of 11 September 2001, to a number of problems affecting its implementation in a more solid manner.

It is, therefore, appropriate to replace this Regulation. The objective is to clarify, simplify and harmonise further the legal requirements with the aim of enhancing the overall security in civil aviation. The new framework regulation should solely lay down the basic principles of what has to be done in order to safeguard civil aviation against acts of unlawful interference, whereas implementing acts should lay down the technical and procedural decisions on how this is to be achieved.

The Commission is of the view that a new regulation will be a clear case and leading example of Better Regulation.

- General context

Regulation (EC) No 2320/2002 was developed as a result of the terrible events of 11 September 2001 in the USA, when four passenger aircraft were hijacked with horrendous consequences. A legislative proposal was thus swiftly drafted and on 16 December 2002 following the procedure under Article 251 of the EC Treaty Regulation (EC) No 2320/2002 laying down basic requirements for aviation security was adopted.

This regulation has now been in force for some 2½ years and has been complemented by implementing legislation, developed through comitology, as envisaged by Articles 4 and 9 of the regulation. It has also had one minor revision - Regulation (EC) No 849/2004 - to rectify some small errors in the original text.

Experience over time has shown that the regulation is too detailed and is in need of simplification. Having such a high degree of detail in framework legislation adopted by co-decision makes legal revision to take into account technical or operational developments impractical. This is an over-prescriptive approach in a framework legislation, which should be replaced by general principles with details added, when necessary, in the implementing legislation.

Whilst recognizing the principle of subsidiarity, the Commission is of the view that a greater degree of harmonization than currently exists of security measures and procedures is desirable. In particular, industry (airlines, cargo shippers and freight forwarders, equipment manufacturers) has a legitimate interest in seeing greater levels of harmonization for facilitation reasons. Indeed, there are situations where facilitation can be achieved through more harmonization without compromising in any way security. In this regard the Commission understands, supports and follows the needs and orientations of industry.

One example where there is a lack of harmonization concerns air cargo security. Point 6.2(b) of the Annex to Regulation (EC) 2320/2002 allows the rules for regulated agents to be defined by the appropriate authority. This has resulted in 25 national systems being in place and a consequential potential distortion of competition and the inability of industry to benefit from the freedoms of the Single Market.

Further harmonization can be developed in greater detail in the implementing legislation. In the example of cargo security it will then be possible to interlink security requirements for

regulated agents and known shippers with the Authorized Economic Operator concept developed in the Community's customs legislation.

Increased harmonization is also an integral element of 'one-stop security' - the concept whereby transfer- and transit passengers, bags and cargo need not be rescreened since there is confidence that baseline levels of security were met at the original departing airport. Again, this is an element that is of benefit to operators acting in a highly competitive market.

In addition to revising the regulation on the grounds of simplification and harmonization, a revision of the regulation can ensure further clarity. The complexity of elements in the regulation has shown that there exists the possibility for different interpretations of the legal requirements. There is also ambiguity in parts of the text. Clarity will contribute to effective implementation of security standards and to legal certainty.

The proposed new regulation would seek to address such issues by improving the overall clarity and legal certainty (and thus quality) of the legislation and, with it, diminish the scope for misinterpretation.

Reference has already been made to the inflexibility that results from having detailed operational and technical standards in co-decision legislation. The Commission is of the view that the ability to (re)act swiftly in the light of risks that are constantly evolving over time is of major significance to improve the overall levels of security. This ability to (re)act swiftly, if necessary, should override potential concerns in relation to the institutional balance for developing legislation. Such an approach is, of course, without prejudice to the scrutiny reserve that the European Parliament has for implementation legislation that is adopted via the comitology process.

Finally, an issue of concern is that the current regulation is in the public domain. Consequently, any amendments made to it will also be in the public domain. In the view of the Commission it is not desirable to have detailed security measures and procedures placed in the public domain, as potential terrorists could use the information to seek out weaknesses in aviation security in order to perpetrate unlawful acts. Similarly, it is also not in the public interest to publicise new developments in security. By placing operational details in implementing legislation this issue can be addressed.

- Existing provisions in the area of the proposal

Regulation (EC) No 2320/2002 of the European Parliament and of the Council establishes common rules in the field of civil aviation security. The proposal seeks to replace this legislative act.

- Consistency with other policies and objectives of the Union

The proposal seeks to replace the existing regulation in order to bring forward better legislation, based on four principles: that of simplification, harmonisation, clarification and enhancing the levels of security.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- Consultation of interested parties

Consultation methods, main sectors targeted and general profile of respondents

The key stakeholder organisations representing airlines, airports, pilots and cargo handlers were all actively involved in a working group that assisted the Commission in developing standards that are reflected in the Commission proposal.

Summary of responses and how they have been taken into account

The stakeholder organisations support, in general terms, the aim of reducing the level of detail in the framework legislation, provided that they can also play an active role in the development of the complementary implementing legislation.

- Collection and use of expertise

There was no need for external expertise.

- Impact assessment

Given that the proposal aims at replacing the existing framework regulation there will be no impact in itself from its adoption. Consequently, dialogue with stakeholder organisations rather than a formal impact assessment was deemed to be most appropriate in the circumstances.

The legislation has no social or environmental impact.

3. LEGAL ELEMENTS OF THE PROPOSAL

- Summary of the proposed action

With one exception it is not the wish of the Commission to change substantively its competences in the field of civil aviation security through a revision of Regulation (EC) No 2320/2002. Rather, what is proposed is a change in the balance of the legislative provisions between those that are laid down in the framework legislation (current Regulation (EC) No 2320/2002, as amended by Regulation (EC) No 849/2003) and those laid down in implementing legislation, of which there are currently seven acts: Commission Regulations (EC) Nos 622/2003, 1217/2003, 1486/2003, 68/2004, 1138/2004, 781/2005 and 857/2005.

Thus, Regulation (EC) No 2320/2002 would be replaced by a simplified, clearer regulation laying down general principles. Those details edited out of the framework legislation would, instead, be introduced into the implementing legislation, which would be amended accordingly.

In this regard it should be noted that the proposal is approximately half the size of the current regulation.

The only additional competence sought relates to rules for in-flight security measures. It covers such diverse topics as access to the cockpit, unruly passengers and in-flight security officers ('sky marshals'). There currently does not exist Community legislation covering in-flight security measures. In the view of the Commission harmonized rules would be best addressed as an element of aviation security legislation, by means of implementing legislation. However, it should be stressed that such implementing legislation will be developed only as and when such rules are deemed necessary at the Community level. Also, it should be noted that the Commission has no intention of compelling any Member State to accept in-flight security officers on board aircraft and the proposal in no way seeks to change existing sovereignty on this matter.

- Legal basis

Article 80(2) of the EC Treaty

- Subsidiarity principle

The subsidiarity principle applies insofar as the proposal does not fall under the exclusive competence of the Community.

The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reason(s).

In view of the Community wide scale of aviation security issues and the very advanced nature of the internal aviation market, the objectives are better achieved at the level of the Community than at national level.

Community action will better achieve the objectives of the proposal for the following reason(s).

The current regulation has already demonstrated why action at community level is the most appropriate.

The current regulation has already demonstrated that a Community approach to aviation security raises both overall standards and mutual confidence between Member States.

As is the case with the existing legislation that this proposal seeks to replace the objectives of the proposed new act are better achieved at the level of the Community in view of the Community-wide scale of aviation security issues and the advanced nature of the internal aviation market.

The proposal therefore complies with the subsidiarity principle.

- Proportionality principle

The proposal complies with the proportionality principle for the following reason(s).

As is the case with the existing legislation, the proposed new act sets common baseline standards, but allows Member States to apply more stringent measures if the threat so warrants.

The proposal does not address the issue of financing security. Who should pay for security - industry or the State - was a major topic of discussion during the adoption of Regulation 2320/2002. The conclusion then was a commitment in an Interinstitutional Declaration that the Commission should undertake a study addressing "in particular the way the financing [of aviation security] is shared between the public authorities and the operators and to submit to the European Parliament and the Council the results and proposals if appropriate". Such a study was undertaken and the results published in September 2004 and placed on the Commission website at http://europa.eu.int/comm/transport/air/safety/studies_en.htm. The report's conclusions are to be used as the basis of a Commission Communication that will look at the funding of security across all modes of transport. This action is foreseen in the 2005 Work Program of the Commission and its intended completion date is the end of 2005. The legislative initiative to replace Regulation 2320/2002 has thus been made without prejudging either the forthcoming Commission communication or the way that security is funded today across the Community.

- Choice of instruments

Proposed instruments: regulation.

Other means would not be adequate for the following reason(s).

The proposal replaces an existing regulation. The regulation was originally deemed the most appropriate instrument a) to ensure uniform application of rules within the Community and b) to ensure the swiftest possible adoption of common rules after the events of 11 September 2001.

4. BUDGETARY IMPLICATION

The proposal has no implication for the Community budget.

5. ADDITIONAL INFORMATION

- Simplification

The proposal provides for simplification of legislation.

Experience over time has shown that Regulation (EC) No 2320/2002 is too detailed and is in need of simplification. Having such a high degree of detail in framework legislation adopted by co-decision makes legal revision to take into account technical or operational developments very impractical.

As an example of this point 4.1.1 of the Annex to the regulation lays down two ways whereby passengers may be screened - by hand or by walk-through-metal-detector. However, in the foreseeable future new technology-based forms of passenger screening will offer a realistic and very accurate alternative way of detecting prohibited items. Unfortunately, technologies other than those described in 4.1.1 of the Annex to the regulation cannot be used for this purpose until the annex is amended accordingly. Given that it requires co-decision procedure this cannot be done swiftly, with potentially negative effects on aviation as a consequence. This is only one example of many.

The adoption of the proposal would lead to the repealing of Regulation 2320/2002 and also Regulation 849/2004 which amended it. The proposal thus follows Commission's commitment to cutting "red tape" by first scrapping existing legislation - the principle of "new for old".

The proposal is included in the Commission's rolling program for up-date and simplification of the acquis communautaire and its Work and Legislative Program under the reference 2005/TREN/016.

- Repeal of existing legislation

The adoption of the proposal will lead to the repeal of existing legislation.

- European Economic Area

The proposed act concerns an EEA matter and should therefore extend to the European Economic Area.

- Detailed explanation of the proposal

Article 1 lays down the objectives, namely establishing common rules for safeguarding civil aviation against acts of unlawful interference. Article 1 does not differ in any significant way from Article 1 of Regulation (EC) No 2320/2002.

Article 2 addresses the scope. The text has been made clearer than in the current regulation to give legal certainty that the regulation applies both to Community airports serving civil aviation, to operators providing services at such airports and to entities performing aviation security functions for flights from such airports (for example catering or cargo facilities that do not lie within the airport perimeter).

Article 3 lays down definitions.

Article 4 refers to the common standards that are to be laid down in Community law, including those measures that should be addressed in implementing legislation.

Article 5 permits Member States to apply more stringent security measures. The principle is unchanged from Article 6 of Regulation (EC) No 2320/2002. However, the new proposal requires that Member States shall both undertake a risk assessment and that they shall be able to justify such action, in general terms, if requested to do so by the Commission. This is to address fears by stakeholders that national authorities can burden industry with additional security requirements without the need to justify their actions. Actions by Member States in response to specific threat information should not be prejudiced by this legislation and so heightened security requirements for individual flights would fall outside the requirements of this article.

Article 6 is new. It addresses the situation whereby a third country requires different security measures on flights from Community airports than those laid down by Community legislation.

Article 7 repeats the requirement (currently contained in Article 5(2) of Regulation (EC) No 2320/2002) that there should be a single authority in each Member State that is responsible for coordinating and monitoring the implementation of the aviation security requirements.

Articles 8-12 require that there shall be security programs at national-, airport- and air carrier level, as well as for all other entities performing aviation security functions. The article is not substantively different from obligations in Articles 5(1) and 5(4) of the existing legislation, but does formally require for the first time in Community legislation a security program by other entities such as cargo handling companies or airline catering companies. The requirement for security programs reflects current best practice in the aviation sector and, as such, is not a significant burden on industry or administrations.

Article 13 lays down an obligation for each Member State to undertake compliance monitoring activities by means of a national quality control program. This article contains the obligations laid down in Articles 5(3) and 7(1) of Regulation (EC) No 2320/2002.

Article 14 allows for Commission inspections of, inter alia, Community airports. It is generally unchanged from the provisions of current Article 7 (2 to 4) of Regulation (EC) No 2320/2002.

Article 15 addresses the dissemination of information.

Article 16 lays down the Committee to assist the Commission in the development of implementing legislation. It is substantively unchanged from Article 9 in Regulation (EC) No 2320/2002.

Article 17 replaces the existing Article 10 on security of flights from third countries. It foresees agreements between the Community and third countries that would allow for the possibility of passengers, bags and cargo transferring at Community airports without the need for rescreening and/or additional security controls.

Article 18 obliges to have penalties against those that fail to adhere to the Community requirements for aviation security. The requirement is unchanged from that currently laid down in Article 12 of Regulation (EC) No 2320/2002.

Articles 19 and 20 repeal the existing regulation and replace it with this new act. It allows a staggered implementation so that existing implementing legislation that complements Regulation (EC) No 2320/2002 can be updated by Committee procedure to bring it into line with the new act so as to avoid a lacuna when the existing Regulation would be repealed.

Turning to the Annex of the new act, this is structured in the same way as the Annex to Regulation (EC) No 2320/2002. However, the contents of each chapter of the Annex have been simplified into general sets of principles. Whilst rules are needed these shall be developed by means of implementing legislation. As an example the new chapter 4 on passengers and cabin baggage is approximately half the size of the existing chapter 4. Only chapter 10 on in-flight security measures did not exist in the current Regulation.

2005/0191 (COD)

Proposal for a

1.3 REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on common rules in the field of civil aviation security (Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 80(2) thereof,

Having regard to the proposal from the Commission[1],

Having regard to the opinion of the European Economic and Social Committee[2],

Having regard to the opinion of the Committee of the Regions[3],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[4],

Whereas:

(1) In order to protect persons and goods within the European Union, acts of unlawful interference with civil aircraft should be prevented by establishing common rules for safeguarding civil aviation. This objective should be achieved by setting common rules and common standards on aviation security as well as mechanisms for monitoring compliance.

(2) It is desirable, in the interests of civil aviation security generally, to provide the basis for a common interpretation of the April 2002 issue of Annex 17 to the Chicago Convention on International Civil Aviation of 7 December 1944.

(3) Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security[5] was adopted as a result of the events of 11 September 2001 in the United States.

(4) The content of Regulation (EC) No 2320/2002 should be revised in the light of the experience gained, and the Regulation itself should be replaced by a new act seeking the simplification, harmonisation and clarification of the existing rules and the improvement of the levels of security.

(5) Given the need for more flexibility in adopting security measures and procedures in order to meet evolving risk assessments and to allow new technologies to be introduced, the new act should lay down the basic principles of what has to be done in order to safeguard civil aviation against acts of unlawful interference without going into technical and procedural details on how they are to be implemented.

(6) The new act should apply to airports serving civil aviation located in the territory of a Member State, to operators providing services at such airports and to entities providing goods and/or services to or through such airports.

(7) Without prejudice to the Convention on offences and certain other acts committed on board aircraft, Tokyo, 1963, the Convention for the suppression of unlawful seizure of aircraft, The Hague, 1970 and the Convention for the suppression of unlawful acts against the safety of civil aviation, Montreal 1971, the new act should cover security measures that apply on board an aircraft, or during a flight, of Community air carriers.

(8) The various types of civil aviation do not necessarily present the same level of threat. In setting common standards on aviation security, the size of the aircraft, the nature of the operation and/or the frequency of operations at airports should be taken into account with a view to permitting the grant of derogations.

(9) Member States should also be allowed, on the basis of a risk assessment, to apply more stringent measures than those to be laid down. However, it should be possible for the Commission to examine those more stringent measures and to decide whether a Member State may continue to apply them.

(10) Third countries may require the application of measures that differ from those laid down in this act in respect of flights from an airport in a Member State to, or over, that third country. However, without prejudice to any bilateral agreements to which the Community is a party, it should be possible for the Commission to examine the measures required by the third country and to decide whether a Member State, operator or other entity concerned may continue to apply the measures required.

(11) Even though, within a single Member State, there may be two or more bodies or entities involved in aviation security, each Member State should designate a single authority responsible for the coordination and monitoring of the implementation of security standards.

(12) In order to define responsibilities for the implementation of the common standards and to describe what measures are required by operators and other entities for this purpose, each

Member State should draw up a national civil aviation security program. Furthermore, each airport operator, air carrier and entity applying aviation security standards should draw up, apply and maintain a security program in order to comply both with the new act and with whichever national civil aviation security program is applicable.

(13) In order to monitor compliance with the new act and with the national civil aviation security program, each Member State should draw up and ensure the implementation of a national program to check the quality of civil aviation security.

(14) In order to monitor the application by Member States of the new act, and also to identify weak points in aviation security, the Commission should conduct inspections, including unannounced inspections.

(15) Implementing acts setting out common measures and procedures for the implementation of the common standards and containing sensitive security information, together with Commission inspection reports and answers of national authorities should be regarded as “EU classified information” within the meaning of Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal rules of procedure[6]. Those items should not be published; they should only be made available to those operators and entities with a legitimate interest.

(16) The measures and procedures necessary for the implementation of this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[7].

(17) For the purpose of allowing transfer passengers and transfer baggage to be exempted from screening when arriving on a flight from a third country, which is known as the concept of “one-stop security”, as well as for allowing passengers arriving on such a flight to mix with screened departing passengers, it is appropriate to encourage agreements between the Community and third countries, recognising that the security standards applied in the third country are equivalent to Community standards.

(18) Penalties should be provided for infringements of the provisions of this Regulation. Those penalties should be effective, proportionate and dissuasive.

HAVE ADOPTED THIS REGULATION:

Article 1

Objectives

1. This Regulation establishes common rules for safeguarding civil aviation against acts of unlawful interference.

It also provides the basis for a common interpretation of the April 2002 issue of Annex 17 to the 1944 Chicago Convention on International Civil Aviation.

2. The means of achieving the objectives set out in paragraph 1 shall be:

- a) the setting of common rules and common standards on aviation security;
- b) mechanisms for monitoring compliance.

Article 2

Scope

This Regulation shall apply to the following:

- a) all airports serving civil aviation located in the territory of a Member State;
- b) all operators, including air carriers, providing services at airports referred to in point (a);
- c) all entities operating from premises located inside or outside airport premises and providing goods and/or services to or through airports referred to in point (a).

Article 3

Definitions

For the purpose of this Regulation:

(1) 'civil aviation' means any air transport operation, both commercial and non-commercial, as well as both scheduled and non-scheduled operations, but excluding operations carried out by state aircraft referred to in Article 3 of the 1944 Chicago Convention on International Civil Aviation;

(2) 'aviation security' means the combination of measures and human and natural resources intended to safeguard civil aviation against acts of unlawful interference;

(3) 'operator' means a person, organisation or enterprise engaged, or offering to engage, in an air transport operation;

(4) 'air carrier' means an air transport undertaking holding a valid operating licence;

(5) 'Community air carrier' means an air carrier holding a valid operating licence granted by a Member State in accordance with Council Regulation (EC) No 2407/92[8];

(6) 'prohibited articles' means weapons, explosives or other dangerous devices, articles or substances that may be used to commit an act of unlawful interference;

(7) 'screening' means the application of technical or other means which are intended to identify and/or detect prohibited articles;

(8) 'security control' means the application of means by which the introduction of prohibited articles may be prevented;

(9) 'access control' means the application of means by which the entry of unauthorised persons or unauthorised vehicles, or both, is prevented;

(10) 'airside' means the movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is restricted;

(11) 'landside' means those parts of an airport, adjacent terrain and buildings or portions thereof that are not airside;

(12) 'security restricted area' means that area of airside where, in addition to access being restricted, access control is applied;

(13) 'demarcated area' means an area that is separated by means of access control either from security restricted areas, or, if the demarcated area itself is a security restricted area, from other security restricted areas of an airport;

(14) 'background check' means a verifiable check of a person's identity, including any criminal history, as part of the assessment of an individual's suitability for unescorted access to security restricted areas;

(15) 'transfer passengers, baggage or cargo' means passengers, baggage or cargo departing on an aircraft other than that on which they arrived;

(16) 'transit passengers, baggage or cargo' means passengers, baggage or cargo departing on the same aircraft as that on which they arrived;

(17) 'potentially disruptive passenger' means a passenger who is either a deportee, a person deemed to be inadmissible for immigration reasons or a person in lawful custody;

(18) 'cabin baggage' means baggage intended for carriage in the cabin of an aircraft;

(19) 'hold baggage' means baggage intended for carriage in the hold of an aircraft;

(20) 'accompanied hold baggage' means baggage accepted for carriage in the hold of an aircraft on which the passenger who checked it in is on board;

(21) 'air carrier mail' means mail whose origin and destination are both an air carrier;

(22) 'air carrier materials' means materials either whose origin and destination are both an air carrier or that are used by an air carrier;

(23) 'cargo' means any property intended for carriage on an aircraft other than baggage, air carrier mail and air carrier materials, and in-flight supplies;

(24) 'regulated agent' means an air carrier, agent, freight forwarder or any other entity who provides the security controls in accordance with this Regulation in respect of cargo;

(25) 'known consignor' means a consignor who originates cargo and whose procedures meet common security rules and standards sufficient to allow carriage of that cargo on any aircraft without further screening;

(26) 'account consignor' means a consignor who originates cargo and whose procedures meet common security rules and standards sufficient to allow carriage of that cargo on all-cargo aircraft without further screening;

(27) 'aircraft check' means an inspection of those parts of the interior of the aircraft to which passengers may have had access, together with an inspection of the hold of the aircraft in order to detect prohibited articles and unlawful interferences with the aircraft;

(28) 'aircraft search' means an inspection of the interior and accessible exterior of the aircraft in order to detect prohibited articles and unlawful interferences with the aircraft;

(29) 'in-flight security officer' means a person who is employed by a Member State to travel on an aircraft of the air carrier licensed by it with the purpose of protecting that aircraft and its occupants against acts of unlawful interference.

Article 4

Common standards

1. The common standards for safeguarding civil aviation against acts of unlawful interference shall be as laid down in the Annex.

2. Detailed measures and procedures for the implementation of the common standards referred to in paragraph 1 shall be laid down in accordance with the procedure referred to in Article 16(2).

These measures shall, in particular, address:

- a) methods of screening, access control and other security controls;
- b) methods of performing aircraft checks and aircraft searches;
- c) prohibited articles;
- d) performance criteria and acceptance tests for equipment;
- e) staff recruitment and training requirements;
- f) the definition of critical parts of security restricted areas;
- g) the obligations of, and the validation procedures for, regulated agents, known consignors and account consignors;
- h) categories of persons and goods that for objective reasons shall be subject to special security procedures or shall be exempted from screening, access control or other security controls.

By way of derogation from the common standards referred to in paragraph 1, the measures and procedures may also address screening, access control or other security controls that provide an adequate level of protection at airports, or demarcated areas thereof. Such alternative measures shall be justified by reasons relating to the size of the aircraft, the nature of the operation and/or the frequency of operations at the airports concerned.

3. Member States shall ensure the application of the common standards referred to in paragraph 1.

Article 5

More stringent measures applied by Member States

1. Member States may apply more stringent measures than the common standards as laid down in Article 4. In doing so, they shall act on the basis of a risk assessment and in compliance with Community law. More stringent measures shall be relevant, objective, non-discriminatory and proportional to the risk that is being addressed.

Member States shall notify the Commission of such measures.

2. The Commission may examine the application of paragraph 1 and, after consulting the Committee referred to in Article 16(1), may decide whether the Member State is allowed to continue to apply the measures.

The Commission shall communicate its decision to the Council and the Member States.

Within one month of the decision being communicated by the Commission, a Member State may refer the decision to the Council. The Council, acting by qualified majority, may within a period of three months take a different decision.

3. The second subparagraph of paragraph 1, and paragraph 2, shall not apply if the more stringent measures are limited to a given flight on a specific date.

Article 6

Security measures required by third countries

1. Without prejudice to any bilateral agreements to which the Community is a party, a Member State shall notify the Commission of measures required by a third country if they differ from the common standards as laid down in Article 4 in respect of flights from an airport in a Member State to, or over, that third country.

2. At the request of the Member State concerned or on its own initiative, the Commission shall examine the application of paragraph 1 and, after consulting the Committee referred to in Article 16(1), may decide whether the Member State, operator or other entity concerned may continue to apply these measures.

The Commission shall communicate its decision to the Council and the Member States.

3. Paragraphs 1 and 2 shall not apply if:

- a) the Member State concerned applies the measures concerned in accordance with Article 5; or
- b) the requirement of the third country is limited to a given flight on a specific date.

Article 7

National authority

Where, within a single Member State, two or more bodies or entities are involved in aviation security, that Member State shall designate a single authority (hereinafter referred to as “the national authority”) to be responsible for the coordination and monitoring of the implementation of the common standards referred to in Article 4.

Article 8

Programs

Member States, airport operators, air carriers and other entities applying aviation security standards shall be responsible for drawing up, applying and maintaining their respective security programs in the manner set out in Articles 9 to 12.

Member States shall additionally perform the broad quality-control function defined in Article 13.

Article 9

National civil aviation security program

1. Every Member State shall draw up, apply and maintain a national civil aviation security program.

That program shall define responsibilities for the implementation of the common standards referred to in Article 4 and shall describe the measures required by operators and other entities for this purpose.

2. The national authority shall make available in writing the appropriate parts of its national civil aviation security program to operators and entities with a legitimate interest.

Article 10

Airport security program

1. Every airport operator shall draw up, apply and maintain an airport security program.

That program shall describe the methods and procedures which are to be followed by the airport operator in order to comply both with this Regulation and with the national civil aviation security program of the Member State in which the airport is located.

The program shall also describe how compliance with these methods and procedures is monitored by the airport operator.

2. The airport security program shall be submitted to the national authority.

Article 11

Air carrier security program

1. Every air carrier shall draw up, apply and maintain an air carrier security program.

That program shall describe the methods and procedures which are to be followed by the air carrier in order to comply both with this Regulation and with the national civil aviation security program of the Member State from which it provides services.

The program shall also describe how compliance with these methods and procedures is monitored by the air carrier.

2. Upon request, the air carrier security program shall be submitted to the national authority.

Article 12

Security program of an entity applying aviation security standards

1. Every entity applying aviation security standards shall draw up, apply and maintain a security program.

That program shall describe the methods and procedures which are to be followed by the entity in order to comply both with this Regulation and with the national civil aviation security program of the Member State in which it is located.

The program shall also describe how compliance with these methods and procedures is to be monitored by the entity itself.

2. Upon request, the security program of the entity applying aviation security standards shall be submitted to the national authority.

Article 13

National quality control program

1. Every Member State shall draw up, and ensure the implementation of, a national quality control program.

That program shall enable the Member State to check the quality of civil aviation security in order to monitor compliance both with this Regulation and with its national civil aviation security program.

2. The specifications for the national quality control program shall be adopted in accordance with the procedure referred to in Article 16(2).

The program shall allow for the swift detection and correction of deficiencies. It shall also provide that all airports, operators and other entities responsible for the application of security standards that are located in the territory of the Member State concerned shall be regularly monitored by, or under the supervision of, the national authority.

Article 14

Commission inspections

1. The Commission, acting in cooperation with the national authority, shall conduct inspections -including inspections of airports, operators and entities applying aviation security standards- in order to monitor the application by Member States of this Regulation and to identify weak points in aviation security. For this purpose, the national authority shall inform the Commission in writing of all airports in its territory serving civil aviation other than those covered by the third subparagraph of Article 4(2).

The procedures for conducting Commission inspections shall be adopted in accordance with the procedure referred to in Article 16(2).

2. Commission inspections of airports, operators and other entities applying aviation security standards shall be unannounced.

3. Each Commission inspection report shall be communicated to the national authority of the Member State concerned, which shall, in its answer, set out the measures taken to remedy any identified deficiencies.

The report, together with the answer of the national authority, shall subsequently be communicated to all other national authorities.

Article 15

Dissemination of information

The following documents shall be regarded as “EU classified documents” for the purposes of Decision 2001/844/EC, ECSC, Euratom, and shall not be placed in the public domain:

- a) measures and procedures as referred to in Article 4(2), if containing sensitive security information;
- b) Commission inspection reports and answers of national authorities, as referred to in Article 14(3).

Article 16

Committee

1. The Commission shall be assisted by a committee (hereinafter referred to as “the Committee”).

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.

The period referred to in Article 5(6) of Decision 1999/468/EC shall be set at one month.

3. The Committee shall adopt its rules of procedure.

Article 17

Third countries

Agreements recognising that the security standards applied in a third country are equivalent to Community standards may be concluded between the Community and a third country in accordance with Article 300 of the Treaty.

Article 18

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

Article 19

Repeal

Regulation (EC) No 2320/2002 is repealed.

Article 20

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union .

It shall apply from [...], with the exception of Articles 4(2), 13(2), 14(1) and 16 which shall apply from the date of entry into force.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament For the Council

The President The President

1.4 COMMON STANDARDS FOR SAFEGUARDING CIVIL AVIATION

COMMON STANDARDS FOR SAFEGUARDING CIVIL AVIATION AGAINST ACTS OF UNLAWFUL INTERFERENCE (ARTICLE 4)

C 300 E/475

Thursday 15 June 2006

1. AIRPORT SECURITY

1.1 Airport planning requirements

1. When designing and constructing new airport facilities or altering existing airport facilities, requirements for the implementation of the common standards referred to in this Annex and implementing acts shall be fully taken into account.

2. At airports the following areas shall be established:

- a) landside;
- b) airside;
- c) security restricted areas; and
- d) critical parts of security restricted areas.

1.2 Access control

1. Access to airside shall be restricted in order to deter unauthorised persons and vehicles from entering these areas.

2. Access to security restricted areas shall be controlled in order to ensure that no unauthorised persons and vehicles enter these areas.

3. Persons and vehicles may only be granted access to airside and security restricted areas if they fulfil the required security conditions.

4. Before being issued with a crew identification card, a flight crew member of a Community air carrier shall have successfully completed a background check carried out by the licensing Member State.

5. Before being issued with an airport identification card that authorises access to security restricted areas, a staff member shall have successfully completed a background check carried out by the Member State in which the airport is located. This shall not apply to flight crew members that have been issued with crew identification cards as referred to in paragraph 4.

1.3 Screening of persons other than passengers and items carried

1. Persons other than passengers, together with items carried, shall be screened on a continuous random basis upon entering security restricted areas in order to prevent prohibited articles from being introduced into these areas.

2. All persons other than passengers, together with items carried, shall be screened upon entering critical parts of security restricted areas in order to prevent prohibited articles from being introduced into these parts.

1.4 Examination of vehicles

Vehicles entering a security restricted area shall be examined in order to prevent prohibited articles from being introduced into these areas.

1.5 Surveillance, patrols and other physical controls

There shall be surveillance, patrols and other physical controls in the security restricted areas and all adjacent areas with public access, in order to identify suspicious behaviour of persons, to identify vulnerabilities which could be exploited to carry out an act of unlawful interference and to deter persons from such acts.

2. DEMARCATED AREAS OF AIRPORTS

Aircraft parked in demarcated areas of airports to which alternative measures referred to in the third subparagraph of Article 4(2) apply, shall be separated from aircraft to which the common standards as laid down in the Annex apply in full, in order to avoid that security standards applied to aircraft, passengers, baggage and cargo of the latter are compromised.

3. AIRCRAFT SECURITY

1. If passengers disembark an aircraft, the aircraft shall be subjected to an aircraft check before departure in order to ensure that no prohibited articles are present on board.

2. Every aircraft shall be protected from unauthorised interference.

3. Every aircraft that has not been protected from unauthorised interference shall be subjected to an aircraft search.

4. PASSENGERS AND CABIN BAGGAGE

4.1 Screening of passengers and cabin baggage

1. All originating, transfer and transit passengers and their cabin baggage shall be screened in order to prevent prohibited articles from being introduced into security restricted areas and on board an aircraft.

2. Transfer passengers and their cabin baggage may be exempted from screening, if:

a) they arrive from a Member State, unless the Commission or that Member State has provided information that those passengers and their cabin baggage cannot be considered as having been screened to the common standards; or

b) they arrive from a third country with which the Community has an agreement as referred to in Article 17 that recognises that these passengers and their cabin baggage have been screened to security standards equivalent to Community standards.

3. Transit passengers and their cabin baggage may be exempted from screening, if:

a) they remain on board the aircraft; or

b) they do not mix with screened departing passengers other than those who board the same aircraft; or

c) they arrive from a Member State, unless the Commission or that Member State has provided information that those passengers and their cabin baggage cannot be considered as having been screened to the common standards; or

d) they arrive from a third country with which the Community has an agreement as referred to in Article 17 that recognises that these passengers and their cabin baggage have been screened to security standards equivalent to Community standards.

4.2 Protection of passengers and cabin baggage

1. Passengers and their cabin baggage shall be protected from unauthorised interference from the point at which they are screened until departure of the aircraft on which they are carried.

2. Screened departing passengers shall not mix with arriving passengers, unless:

a) the passengers arrive from a Member State, provided that the Commission or that Member State has not provided information that those arriving passengers and their cabin baggage cannot be considered as having been screened to the common standards; or

b) the passengers arrive from a third country with which the Community has an agreement as referred to in Article 17 that recognises that these passengers have been screened to security standards equivalent to Community standards.

4.3 Potentially disruptive passengers

Before departure potentially disruptive passengers shall be subjected to appropriate security measures.

5. HOLD BAGGAGE

5.1 Screening of hold baggage

1. All hold baggage shall be screened prior to being loaded onto an aircraft.

2. Transfer hold baggage may be exempted from screening, if:

a) it arrives from a Member State, unless the Commission or that Member State has provided information that this hold baggage cannot be considered as having been screened to the common standards; or

b) it arrives from a third country with which the Community has an agreement as referred to in Article 17 that recognises that this hold baggage has been screened to security standards equivalent to Community standards.

3. Transit hold baggage may be exempted from screening if it remains on board the aircraft.

5.2 Protection of hold baggage

Hold baggage to be carried on an aircraft shall be protected from unauthorised interference from the point at which it is screened or accepted into the care of the air carrier, whichever is earlier, until the departure of the aircraft on which it is to be carried.

5.3 Baggage reconciliation

1. Each item of hold baggage shall be identified as accompanied or unaccompanied. The hold baggage of a passenger who has checked in for a flight but who is not on board the aircraft shall be identified as unaccompanied.

2. Unaccompanied hold baggage shall not be transported, unless that baggage has been either separated due to factors beyond the passenger's control or subjected to additional security controls.

6. CARGO

6.1 Security controls for cargo

1. All cargo shall be subjected to security controls prior to being loaded on an aircraft. An air carrier shall not accept cargo for carriage on an aircraft unless the application of security controls is confirmed and accounted for by a regulated agent, a known consignor or an account consignor.

2. Transfer cargo shall be subjected to security controls as detailed in an implementing act.

3. Transit cargo may be exempted from security controls if it remains on board the aircraft.

6.2 Protection of cargo

1. Cargo to be carried on an aircraft shall be protected from unauthorised interference from the point at which security controls are applied until the departure of the aircraft on which it is to be carried.

2. Cargo that is not adequately protected from unauthorised interference after security controls have been applied shall be screened.

7. AIR CARRIER MAIL AND AIR CARRIER MATERIALS

Air carrier mail and air carrier materials shall be subjected to security controls and thereafter protected until loaded onto the aircraft in order to prevent prohibited articles from being introduced on board an aircraft.

8. IN-FLIGHT SUPPLIES

In-flight supplies, including catering, intended for carriage or use on board an aircraft shall be subjected to security controls and thereafter protected until loaded onto the aircraft in order to prevent prohibited articles from being introduced on board an aircraft.

9. AIRPORT SUPPLIES

Supplies intended to be sold or used in security restricted areas of airports, including supplies for duty-free shops and restaurants, shall be subjected to security controls in order to prevent prohibited articles from being introduced into these areas.

10. IN-FLIGHT SECURITY MEASURES

1. Without prejudice to the applicable aviation safety rules, unauthorised persons shall be prevented from entering the flight crew compartment during a flight.

2. Without prejudice to the applicable aviation safety rules, potentially disruptive passengers shall be subjected to appropriate security measures during a flight.

3. If, during a flight, a passenger seeks to commit an act of unlawful interference, appropriate security measures shall be taken to prevent such an act.

4. Weapons shall not be carried on board an aircraft, unless an authorisation has been given by the Member State concerned and the required security conditions have been fulfilled.

5. In-flight security officers may only be deployed on board an aircraft if the required security conditions and training have been fulfilled. Member States retain the right not to authorise the use of in-flight security officers on flights of air carriers licensed by them.

6. Paragraphs 1 to 5 shall apply only to Community air carriers.

11. STAFF RECRUITMENT AND TRAINING

1. Persons implementing, or responsible for implementing, screening, access control or other security controls shall be recruited, trained and certified so as to ensure that they are suitable for employment and competent to undertake the duties to which they will be assigned.

2. Persons other than passengers requiring access to security restricted areas shall, before either an airport identification card or crew identification card is issued, receive security training.

3. Training as referred to in paragraphs 1 and 2 shall be conducted on initial and recurrent basis.

4. Instructors engaged in the training of the persons mentioned in paragraphs 1 and 2 shall be qualified.

12. SECURITY EQUIPMENT

Equipment used for screening, access control and other security controls shall be capable to perform the security controls concerned.

[1] OJ C [...], [...], p. [...].

[2] OJ C [...], [...], p. [...].

[3] OJ C [...], [...], p. [...].

[4] OJ C [...], [...], p. [...].

[5] OJ L 355, 30.12.2002, p. 1.

[6] OJ L 317, 3.12.2001, p. 1.

[7] OJ L 184, 17.7.1999, p. 23.

[8] OJ L 240, 24.8.1992, p. 1.

1.5 Directive 95/46/EC

Directive 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

Official Journal L 281 , 23/11/1995 P. 0031 – 0050

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must

be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the

processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be

carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related

purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary or artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial

interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for

consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. **Member States** shall prohibit the processing of 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.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) 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.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

- (a) the identity of the controller and of his representative, if any;
- (b) the purposes of the processing for which the data are intended;
- (c) any further information such as
 - the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide

information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred

on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. In that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are

incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20

February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.

1.6 Directive 97/66

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Official Journal L 024 , 30/01/1998 P. 0001 - 0008

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure laid down in Article 189b of the Treaty (3), in the light of the joint text approved by the Conciliation Committee on 6 November 1997,

(1) Whereas 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 (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community;

(2) Whereas confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights (in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms) and the constitutions of the Member States;

(3) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterised by the introduction of new telecommunications services; whereas the

successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(4) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(5) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (5), called for steps to be taken to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasised the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992 (6);

(6) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(7) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users;

(8) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the telecommunications sector, must be harmonised in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 7a of the Treaty; whereas the harmonisation is limited to requirements that are necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

(9) Whereas the Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant

technologies where this is necessary to apply the guarantees provided for by the provisions of this Directive.

(10) Whereas these new services include interactive television and video on demand;

(11) Whereas, in the telecommunications sector, in particular for all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunications services;

(12) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;

(13) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons; whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons; whereas this protection is ensured within the framework of the applicable Community and national legislation;

(14) Whereas the application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges must not be made mandatory in specific cases where such application would prove to be technically impossible or would require a

disproportionate economic effort; whereas it is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission;

(15) Whereas service providers must take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network; whereas security is appraised in the light of the provision of Article 17 of Directive 95/46/EC;

(16) Whereas measures must be taken to prevent the unauthorised access to communications in order to protect the confidentiality of communications by means of public telecommunications networks and publicly available telecommunications services; whereas national legislation in some Member States only prohibits intentional unauthorized access to communications;

(17) Whereas the data relating to subscribers processed to establish calls contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons; whereas such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time; whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications services may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available telecommunications services about the types of further processing he intends to perform;

(18) Whereas the introduction of itemized bills has improved the possibilities for the subscriber to verify the correctness of the fees charged by the service provider; whereas, at the same time, it may jeopardise the privacy of the users of publicly available telecommunications services; whereas therefore, in order to preserve the privacy of the user, Member States must encourage the development of telecommunications service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available telecommunications services, for example calling cards and facilities for payment by credit card; whereas, alternatively, Member States may, for the same purpose, require the deletion of a certain number of digits from the called numbers mentioned in itemized bills;

(19) Whereas it is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines; whereas it is justified to override the elimination of calling line identification presentation in specific cases; whereas certain subscribers, in particular helplines and similar organizations, have an interest in guaranteeing the anonymity of their callers; whereas it is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls; whereas the providers of publicly available telecommunications services must inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification and about the privacy options which are available; whereas this will allow the subscribers to make an informed choice about the privacy facilities they may want to use; whereas the privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available telecommunications service;

(20) Whereas safeguards must be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others; whereas, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available telecommunications service;

(21) Whereas directories are widely distributed and publicly available; whereas the right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine the extent to which their personal data are published in a directory; whereas Member States may limit this possibility to subscribers who are natural persons;

(22) Whereas safeguards must be provided for subscribers against intrusion into their privacy by means of unsolicited calls and telefaxes; whereas Member States may limit such safeguards to subscribers who are natural persons;

(23) Whereas it is necessary to ensure that the introduction of technical features of telecommunications equipment for data protection purposes is harmonised in order to be compatible with the implementation of the internal market;

(24) Whereas in particular, similarly to what is provided for by Article 13 of Directive 95/46/EC, Member States can restrict the scope of subscribers' obligations and rights in certain circumstances, for example by ensuring that the provider of a publicly available telecommunications service may override the elimination of the presentation of calling line identification in conformity with national legislation for the purpose of prevention or detection of criminal offences or State security;

(25) Whereas where the rights of the users and subscribers are not respected, national legislation must provide for judicial remedy; whereas sanctions must be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive;

(26) Whereas it is useful in the field of application of this Directive to draw on the experience of the Working Party on the protection of individuals with regard to the processing of personal data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC;

(27) Whereas, given the technological developments and the attendant evolution of the services on offer, it will be necessary technically to specify the categories of data listed in the Annex to this Directive for the application of Article 6 of this Directive with the assistance of the Committee composed of representatives of the Member States set up in Article 31 of Directive 95/46/EC in order to ensure a coherent application of the requirements set out in this Directive regardless of changes in technology; whereas this procedure applies solely to specifications necessary to adapt the Annex to new technological developments, taking into consideration changes in market and consumer demand; whereas the Commission must duly inform the European Parliament of its intention to apply this procedure and whereas, otherwise, the procedure laid down in Article 100a of the Treaty shall apply;

(28) Whereas, to facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1 Object and scope

1. This Directive provides for the harmonisation of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2 Definitions

In addition to the definitions given in Directive 95/46/EC, for the purposes of this Directive:

(a) 'subscriber` shall mean any natural or legal person who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services;

(b) 'user` shall mean any natural person using a publicly available telecommunications service, for private or business purposes, without necessarily having subscribed to this service;

(c) 'public telecommunications network` shall mean transmission systems and, where applicable, switching equipment and other resources which permit the conveyance of signals between defined termination points by wire, by radio, by optical or by other electromagnetic means, which are used, in whole or in part, for the provision of publicly available telecommunications services;

(d) 'telecommunications service' shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting.

Article 3 Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks in the Community, in particular via the Integrated Services Digital Network (ISDN) and public digital mobile networks.

2. Articles 8, 9 and 10 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate investment to fulfil the requirements of Articles 8, 9 and 10 shall be notified to the Commission by the Member States.

Article 4 Security

1. The provider of a publicly available telecommunications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5 Confidentiality of the communications

1. Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised, in accordance with Article 14 (1).

2. Paragraph 1 shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Article 6 Traffic and billing data

1. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.

2. For the purpose of subscriber billing and interconnection payments, data indicated in the Annex may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.

3. For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

4. Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.

5. Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

Article 7 Itemized billing

1. Subscribers shall have the right to receive non-itemized bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative modalities for communications or payments are available to such users and subscribers.

Article 8 Presentation and restriction of calling and connected line identification

1. Where presentation of calling-line identification is offered, the calling user must have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling-line identification is offered, the called subscriber must have the possibility via a simple means, free of charge for reasonable use of this function, to prevent the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the called subscriber must have the possibility via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the called subscriber must have the possibility via a simple means, free of charge, to eliminate the presentation of the connected line identification to the calling user.

5. The provisions set out in paragraph 1 shall also apply with regard to calls to third countries originating in the Community; the provisions set out in paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available telecommunications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9 Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available telecommunications service may override the elimination of the presentation of calling line identification:

(a) on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls; in this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public telecommunications network and/or publicly available telecommunications service;

(b) on a per-line basis for organisations dealing with emergency calls and recognized as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of answering such calls.

Article 10 Automatic call forwarding

Member States shall ensure that any subscriber is provided, free of charge and via a simple means, with the possibility to stop automatic call forwarding by a third party to the subscriber's terminal.

Article 11 Directories of subscribers

1. Personal data contained in printed or electronic directories of subscribers available to the public or obtainable through directory enquiry services should be limited to what is necessary to identify a particular subscriber, unless the subscriber has given his unambiguous consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, to be omitted from a printed or electronic directory at his or her request, to indicate that his or her personal data may not be used for the purpose of direct marketing, to have his or her address omitted in part and not to have a reference revealing his or her sex, where this is applicable linguistically.

2. Notwithstanding paragraph 1, Member States may allow operators to require a payment from subscribers wishing to ensure that their particulars are not entered in a directory, provided that the sum involved does not act as a disincentive to the exercise of this right, and that, taking account of the quality requirements of the public directory in the light of the universal service, it is limited to the actual costs incurred by the operator for the adaptation and updating of the list of subscribers not to be included in the public directory.

3. The rights conferred by paragraph 1 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 12 Unsolicited calls

1. The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Member States shall take appropriate measures to ensure that, free of charge, unsolicited calls for purposes of direct marketing, by means other than those referred to in paragraph 1, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls, the choice between these options to be determined by national legislation.

3. The rights conferred by paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.

Article 13 Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other telecommunications equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features, Member States shall inform the Commission according to the procedures provided for by Directive 83/189/EEC (7) which lays down a procedure for the provision of information in the field of technical standards and regulations.

3. Where required, the Commission will ensure the drawing up of common European standards for the implementation of specific technical features, in accordance with Community legislation on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and telecommunications (8).

Article 14 Extension of the scope of application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6 and Article 8(1), (2), (3) and (4), when such restriction constitutes a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system, as referred to in Article 13(1) of Directive 95/46/EC.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data established according to Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the telecommunications sector, which is the subject of this Directive.

4. The Commission, assisted by the Committee established by Article 31 of Directive 95/46/EC, shall technically specify the Annex according to the procedure mentioned in this Article. The aforesaid Committee shall be convened specifically for the subjects covered by this Directive.

Article 15 Implementation of the Directive

1. Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with this Directive not later than 24 October 1998.

By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary for them to comply with Article 5 of this Directive not later than 24 October 2000.

When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference at the time of their official publication. The procedure for such reference shall be adopted by Member States.

2. By way of derogation from Article 6(3), consent is not required with respect to processing already under way on the date the national provisions adopted pursuant to this Directive enter into force. In those cases the subscribers shall be informed of this processing and if they do not express their dissent within a period to be determined by the Member State, they shall be deemed to have given their consent.

3. Article 11 shall not apply to editions of directories which have been published before the national provisions adopted pursuant to this Directive enter into force.

4. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive.

Article 16 Addressees

This Directive is addressed to the Member States.

Done at Brussels, 15 December 1997.

For the European Parliament

The President

J. M. GIL-ROBLES

For the Council

The President

J.-C. JUNCKER

(1) OJ C 200, 22.7.1994, p. 4.

(2) OJ C 159, 17.6.1991, p. 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ C 94, 13.4.1992, p. 198). Council Common Position of 12 September 1996 (OJ C 315, 24.10.1996, p. 30) and Decision of the European Parliament of 16 January 1997 (OJ C 33, 3.2.1997, p. 78). Decision of the European Parliament of 20 November 1997 (OJ C 371, 8.12.1997). Council Decision of 1 December 1997.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ C 257, 4.10.1988, p. 1.

(6) OJ C 196, 1.8.1989, p. 4.

(7) OJ L 109, 26.4.1983, p. 8. Directive as last amended by Directive 94/10/EC (OJ L 100, 19.4.1994, p. 30).

(8) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

ANNEX

List of data

For the purpose referred to in Article 6(2) the following data may be processed:

Data containing the:

- number or identification of the subscriber station,
- address of the subscriber and the type of station,
- total number of units to be charged for the accounting period,
- called subscriber number,
- type, starting time and duration of the calls made and/or the data volume transmitted,
- date of the call/service,
- other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.

1.7 Directive 2002/58

Official Journal L 201 , 31/07/2002 P. 0037 - 0047

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission(1),

Having regard to the opinion of the Economic and Social Committee(2),

Having consulted the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(3),

Whereas:

(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(4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.

(3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States.

(4) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector⁽⁵⁾ translated the principles set out in Directive 95/46/EC into specific rules for the telecommunications sector. Directive 97/66/EC has to be adapted to developments in the markets and technologies for electronic communications services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

(6) The Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.

(7) In the case of public communications networks, specific legal, regulatory and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.

(8) Legal, regulatory and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interest of legal persons, in the electronic communication sector, should be harmonised in order to avoid obstacles to the internal market for electronic communication in accordance with Article 14 of the Treaty. Harmonisation should be limited to requirements necessary to guarantee that the promotion and development of new electronic communications services and networks between Member States are not hindered.

(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible.

(10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

(11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(12) Subscribers to a publicly available electronic communications service may be natural or legal persons. By supplementing Directive 95/46/EC, this Directive is aimed at protecting the

fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons. This Directive does not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons, which is ensured within the framework of the applicable Community and national legislation.

(13) The contractual relation between a subscriber and a service provider may entail a periodic or a one-off payment for the service provided or to be provided. Prepaid cards are also considered as a contract.

(14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

(15) A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.

(16) Information that is part of a broadcasting service provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However, in cases where the individual subscriber or user receiving such information can be identified, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.

(17) For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data

subject's consent as defined and further specified in Directive 95/46/EC. Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website.

(18) Value added services may, for example, consist of advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.

(19) The application of certain requirements relating to presentation and restriction of calling and connected line identification and to automatic call forwarding to subscriber lines connected to analogue exchanges should not be made mandatory in specific cases where such application would prove to be technically impossible or would require a disproportionate economic effort. It is important for interested parties to be informed of such cases and the Member States should therefore notify them to the Commission.

(20) Service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. It is particularly important for subscribers and users of such services to be fully informed by their service provider of the existing security risks which lie outside the scope of possible remedies by the service provider. Service providers who offer publicly available electronic communications services over the Internet should inform users and subscribers of measures they can take to protect the security of their communications for instance by using specific types of software or encryption technologies. The requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. The provision of information about security risks to the subscriber should be free of charge except for any nominal costs which the subscriber may incur while receiving or collecting the information, for instance by downloading an electronic mail message. Security is appraised in the light of Article 17 of Directive 95/46/EC.

(21) Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications, by means of public communications networks and publicly available

electronic communications services. National legislation in some Member States only prohibits intentional unauthorised access to communications.

(22) The prohibition of storage of communications and the related traffic data by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

(23) Confidentiality of communications should also be ensured in the course of lawful business practice. Where necessary and legally authorised, communications can be recorded for the purpose of providing evidence of a commercial transaction. Directive 95/46/EC applies to such processing. Parties to the communications should be informed prior to the recording about the recording, its purpose and the duration of its storage. The recorded communication should be erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged.

(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying

the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

(26) The data relating to subscribers processed within electronic communications networks to establish connections and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

(27) The exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service that is provided. For instance for a voice telephony call the transmission will be completed as soon as either of the users terminates the connection. For

electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.

(28) The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services.

(29) The service provider may process traffic data relating to subscribers and users where necessary in individual cases in order to detect technical failure or errors in the transmission of communications. Traffic data necessary for billing purposes may also be processed by the provider in order to detect and stop fraud consisting of unpaid use of the electronic communications service.

(30) Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required.

(31) Whether the consent to be obtained for the processing of personal data with a view to providing a particular value added service should be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it.

(32) Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in Directive 95/46/EC. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card. To the same end, Member States may ask the operators to offer their subscribers a different type of detailed bill in which a certain number of digits of the called number have been deleted.

(34) It is necessary, as regards calling line identification, to protect the right of the calling party to withhold the presentation of the identification of the line from which the call is being made and the right of the called party to reject calls from unidentified lines. There is justification for overriding the elimination of calling line identification presentation in specific cases. Certain subscribers, in particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. It is necessary, as regards connected line identification, to protect the right and the legitimate interest of the called party to withhold the presentation of the identification of the line to which the calling party is actually connected, in particular in the case of forwarded calls. The providers of publicly available electronic communications services should inform their subscribers of the existence of calling and connected line identification in the network and of all services which are offered on the basis of calling and connected line identification as well as the privacy options which are available. This will allow the subscribers to make an informed choice about the privacy facilities they may want to use. The privacy options which are offered on a per-line basis do not necessarily have to be available as an automatic network service but may be obtainable through a simple request to the provider of the publicly available electronic communications service.

(35) In digital mobile networks, location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications. Such data are traffic data covered by Article 6 of this Directive. However, in addition, digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have

given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge.

(36) Member States may restrict the users' and subscribers' rights to privacy with regard to calling line identification where this is necessary to trace nuisance calls and with regard to calling line identification and location data where this is necessary to allow emergency services to carry out their tasks as effectively as possible. For these purposes, Member States may adopt specific provisions to entitle providers of electronic communications services to provide access to calling line identification and location data without the prior consent of the users or subscribers concerned.

(37) Safeguards should be provided for subscribers against the nuisance which may be caused by automatic call forwarding by others. Moreover, in such cases, it must be possible for subscribers to stop the forwarded calls being passed on to their terminals by simple request to the provider of the publicly available electronic communications service.

(38) Directories of subscribers to electronic communications services are widely distributed and public. The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.

(39) The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion. Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.

(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

(41) Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC. When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

(42) Other forms of direct marketing that are more costly for the sender and impose no financial costs on subscribers and users, such as person-to-person voice telephony calls, may justify the maintenance of a system giving subscribers or users the possibility to indicate that they do not want to receive such calls. Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems, only allowing such calls to subscribers and users who have given their prior consent.

(43) To facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

(44) Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from

downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

(45) This Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an opt-out register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce)(6) are fully applicable.

(46) The functionalities for the provision of electronic communications services may be integrated in the network or in any part of the terminal equipment of the user, including the software. The protection of the personal data and the privacy of the user of publicly available electronic communications services should be independent of the configuration of the various components necessary to provide the service and of the distribution of the necessary functionalities between these components. Directive 95/46/EC covers any form of processing of personal data regardless of the technology used. The existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way. It may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity(7) will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market.

(47) Where the rights of the users and subscribers are not respected, national legislation should provide for judicial remedies. Penalties should be imposed on any person, whether governed by private or public law, who fails to comply with the national measures taken under this Directive.

(48) It is useful, in the field of application of this Directive, to draw on the experience of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data composed of representatives of the supervisory authorities of the Member States, set up by Article 29 of Directive 95/46/EC.

(49) To facilitate compliance with the provisions of this Directive, certain specific arrangements are needed for processing of data already under way on the date that national implementing legislation pursuant to this Directive enters into force,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope and aim

1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Definitions

Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)(8) shall apply.

The following definitions shall also apply:

(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

(e) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

(f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;

(g) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Article 3

Services concerned

1. This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

2. Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges.

3. Cases where it would be technically impossible or require a disproportionate economic effort to fulfil the requirements of Articles 8, 10 and 11 shall be notified to the Commission by the Member States.

Article 4

Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 5

Confidentiality of the communications

1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Article 6

Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.

4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.

5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

Article 7

Itemised billing

1. Subscribers shall have the right to receive non-itemised bills.

2. Member States shall apply national provisions in order to reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, for example by ensuring that sufficient alternative privacy enhancing methods of communications or payments are available to such users and subscribers.

Article 8

Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.

5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.

6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility,

using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Article 10

Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

(a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;

(b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11

Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 12

Directories of subscribers

1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected.

Article 13

Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a

service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

Article 14

Technical features and standardisation

1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission in accordance with the procedure provided for by Directive 98/34/EC of the European Parliament and

of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services(9).

3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications(10).

Article 15

Application of certain provisions of Directive 95/46/EC

1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

2. The provisions of Chapter III on judicial remedies, liability and sanctions of Directive 95/46/EC shall apply with regard to national provisions adopted pursuant to this Directive and with regard to the individual rights derived from this Directive.

3. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC shall also carry out the tasks laid down in Article 30 of that Directive with regard to matters covered by this Directive, namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector.

Article 16

Transitional arrangements

1. Article 12 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this Directive enter into force.

2. Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the provisions of Directive 95/46/EC and of Article 11 of Directive 97/66/EC before the national provisions adopted in pursuance of this Directive enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 12 of this Directive.

Article 17

Transposition

1. Before 31 October 2003 Member States shall bring into force the provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the provisions of national law which they adopt in the field governed by this Directive and of any subsequent amendments to those provisions.

Article 18

Review

The Commission shall submit to the European Parliament and the Council, not later than three years after the date referred to in Article 17(1), a report on the application of this Directive and its impact on economic operators and consumers, in particular as regards the provisions on unsolicited communications, taking into account the international environment. For this purpose, the Commission may request information from the Member States, which shall be supplied without undue delay. Where appropriate, the Commission shall submit proposals to amend this Directive, taking account of the results of that report, any changes in the sector and any other proposal it may deem necessary in order to improve the effectiveness of this Directive.

Article 19

Repeal

Directive 97/66/EC is hereby repealed with effect from the date referred to in Article 17(1).

References made to the repealed Directive shall be construed as being made to this Directive.

Article 20

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities.

Article 21

Addressees

This Directive is addressed to the Member States.

Done at Brussels, 12 July 2002.

For the European Parliament

The President

P. Cox

For the Council

The President

T. Pedersen

(1) OJ C 365 E, 19.12.2000, p. 223.

(2) OJ C 123, 25.4.2001, p. 53.

(3) Opinion of the European Parliament of 13 November 2001 (not yet published in the Official Journal), Council Common Position of 28 January 2002 (OJ C 113 E, 14.5.2002, p. 39) and Decision of the European Parliament of 30 May 2002 (not yet published in the Official Journal). Council Decision of 25 June 2002.

(4) OJ L 281, 23.11.1995, p. 31.

(5) OJ L 24, 30.1.1998, p. 1.

(6) OJ L 178, 17.7.2000, p. 1.

(7) OJ L 91, 7.4.1999, p. 10.

(8) OJ L 108, 24.4.2002, p. 33.

(9) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(10) OJ L 36, 7.2.1987, p. 31. Decision as last amended by the 1994 Act of Accession.

1.8 PETs Privacy Enhancing Technologies

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs) (Text with EEA relevance)

1. INTRODUCTION

The intensive and sustained development of information and communication technologies (ICT) is constantly offering new services which improve people's life. To a large extent, the raw material for interactions in cyberspace is the personal data of individuals moving around in it when they purchase goods and services, establish or maintain contact with others or communicate their ideas on the world wide web. Alongside the benefits brought about by these developments, new risks also arise for the individual, such as identity theft, discriminatory profiling, continuous surveillance or fraud.

The Charter of Fundamental Rights of the European Union recognises in Article 8 the right to the protection of personal data. This fundamental right is set forth in a European legal framework on the protection of personal data consisting in particular of the Data Protection Directive 95/46/EC¹ and the ePrivacy Directive 2002/58/EC² as well as the Data Protection Regulation (EC) 45/2001³ relating to processing by Community institution and bodies. This legislation lays down several substantive provisions imposing obligations on data controllers and recognizing rights of data subjects. It also prescribes sanctions and appropriate remedies in cases of breach and establishes enforcement mechanisms to make them effective.

However, this system may prove insufficient when personal data is disseminated worldwide through ICT networks and the processing of data crosses several jurisdictions, often outside the EU. In such situations the current rules may be considered to apply and to provide a clear legal response. Furthermore, a competent authority to enforce the rules may also be identified. However, considerable practical obstacles may exist as a result of difficulties with the technology used involving data processing by different actors in different locations and there may be hurdles intrinsic to the enforcement of national administrative and court rulings in another jurisdiction, especially in non-EU countries.

Whilst strictly speaking data controllers bear the legal responsibility for complying with data protection rules, others also bear some responsibility for data protection from a societal and ethical point of view. These involve those who design technical specifications and those who actually build

or implement applications or operating systems. Article 17 of the Data Protection Directive lays down the data controller's obligation to implement appropriate technical and organisational measures and to ensure a level of security appropriate to the nature of the data and the risks of processing it. The use of technology to support the respect for legislation, in particular the data protection rules, is already envisaged to some extent in the ePrivacy Directive.

A further step to pursue the aim of the legal framework, whose objective is to minimise the processing of personal data and using anonymous or pseudonymous data where possible, could be supported by measures called Privacy Enhancing Technologies or PETs - that would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult.

The purpose of this Communication, which follows from the First Report on the implementation of the Data Protection Directives, is to consider the benefits of PETs, lay down the Commission's objectives in this field to promote these technologies, and set out clear actions to achieve this goal by supporting the development of PETs and their use by data controllers and consumers.

2. WHAT ARE PETs?

There are a number of definitions of PETs used by the academic community and by pilot projects on this matter. For instance, according to the EC-funded PISA project, PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system. The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The Commission in its First Report on the implementation of the Data Protection Directive considers that "...the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy *protection*...". The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them.

In the dynamic landscape of ICT, the effectiveness of different PETs to ensure the protection of privacy, including aspects of compliance with data protection law, is varied and changes over time. Their typology is also varied. They can be stand-alone tools requiring positive action by

consumers (who must purchase and install them in their PCs) or be built into the very architecture of information systems. Several examples of PETs can be mentioned here:

Automatic anonymisation of data, after a certain lapse of time, supports the principle that processed data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected.

3. THE COMMISSION SUPPORTS PETS

The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfil data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms.

In its Communication on a strategy for a secure Information Society, COM(2006) 251 of 31 May 2006, the Commission invited in particular the private sector to "*stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy-intrusive attacks*". Furthermore, in the Commission's Roadmap for a pan-European eIDM Framework by 2010, one of the key principles governing electronic identity management is that "the system must be secure, implement the necessary safeguards to protect the user's privacy, and allow its usage to be aligned with local interest and sensitivities".

The intervention of different actors in data processing and the existence of different national jurisdictions involved could make enforcement of the legal framework difficult. On the other hand, PETs could ensure that certain breaches of data protection rules, resulting in invasions of fundamental rights including privacy, could be avoided because they would become technologically more difficult to carry out. The Commission is aware of the fact that technology – although having a crucial role in privacy protection – is not sufficient in itself to secure privacy. PETs need to be applied according to a regulatory framework of enforceable data protection rules providing a number of negotiable levels of privacy protection for all individuals. The use of PETs does not mean that operators can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data).

Important public interests could also be better served. The data protection legal framework provides for restrictions to the general principles and interference in the rights of individuals for important public interests such as public security, the fight against crime or public health. The conditions for such restrictions are laid down in Article 13 of the Data Protection Directive and Article 15 of the ePrivacy Directive. They are substantially similar to those set by Article 8 of the European Convention on Human Rights (ECHR), namely that such interference is done in accordance with the law and is proportionate and necessary in a democratic society for a legitimate public purpose⁷. The use of PETs should not prevent law enforcement agencies or other competent authorities from intervening in the lawful exercise of their functions for an important public interest, e.g. fighting cybercrime, combating terrorism or preventing the spread of contagious diseases. The responsible authorities should be in a position to access personal data where necessary to achieve those purposes and in accordance with the procedures, conditions and safeguards laid down by the law.

Better respect of data protection rules would also have a positive impact on consumer trust, in particular in cyberspace. A number of promising and value-added services that rely on transfers of personal data across IT-Networks, such as e-learning, e-government, e-health, ebanking, e-commerce or "intelligent car" systems would certainly benefit. People could be sure that the data they are providing to identify themselves, receive services or make payments will only be used for legitimate purposes and that their participation in the digital community is not done at the expense of sacrificing their rights.

4. WORK DONE AND THE WAY FORWARD

To pursue the objective of enhancing the level of privacy and data protection in the Community by, among others, promoting the development and the use of PETs, the Commission intends to conduct the following activities, involving a vast array of actors, including its own services, national authorities, industry and consumers.

In these discussions attention will be given to the specific situation of small and medium-sized enterprises (SMEs) and the possibilities or incentives for their use of PETs. The Commission should also, among other issues, consider trust and awareness - issues which are of particular importance to SMEs.

4.1. First objective: to support the development of PETs

If PETs are to be widely used, there needs to be further design, development and manufacturing of PETs. Whilst these activities are already done to a certain degree by the public and private sector the Commission considers that these activities should be stepped up. With this aim in mind, the need for PETs and their technological requirements should be identified and RTD activities should develop the tools.

4.1.1. Action 1.1.: Identifying the need and technological requirements of PETs

PETs are heavily dependent on the evolution of ICT. Once the dangers posed by technological developments are detected, the appropriate requirements for a technological solution must be identified.

The Commission will encourage various stakeholder groups to come together and debate PETs. These groups will include in particular representatives from the ICT sector, PETs developers, data protection authorities, law enforcement bodies, technology partners including experts from relevant fields, such as eHealth or information security, consumers and civil rights associations. These stakeholders should regularly look into the evolution of technology, detect the dangers it poses to fundamental rights and data protection, and outline the technical requirements of a PETs response. This may include fine-tuning the technological measures in accordance with the different risks and the different data at stake and taking into account the need to safeguard public interests, such as public security.

4.1.2. Action 1.2.: Developing PETs

As the need for and technological requirements of PETs are identified, concrete action has to be taken to arrive at an end-product ready to use. The Commission has already addressed the need for PETs. Under the auspices of the 6th Framework Program it sponsors the PRIME₈ project tackling issues of digital identity management and privacy in the information society. The OPEN-TC₉ project will allow privacy protection based on open trusted computing and the DISCREET₁₀ project develops middleware to enforce privacy in advanced network services. In the future, under the 7th Framework Program, the Commission intends to support other RTD projects and largescale pilot demonstrations to develop and stimulate the uptake of PETs. The aim is to provide the foundation for user-empowering privacy protection services reconciling legal and technical differences across Europe through public-private partnerships.

The Commission also calls on national authorities and on the private sector to invest in the development of PETs. Such investment is key to placing European industry ahead in a sector that will grow as these technologies become increasingly required by technological standards and by consumers more aware of the need to protect their rights in cyberspace.

4.2. Second objective: to support the use of available PETs by data controllers

PETs will only be truly beneficial if they are effectively incorporated into and used by technical equipment and software tools that carry out processing of personal data. The participation of the industry that manufactures such equipment and of data controllers who avail themselves of it to carry out data processing activities is therefore paramount.

4.2.1. Action 2.1.: Promoting the use of PETs by industry

The Commission believes that all those involved in processing of personal data would benefit from a wider use of PETs. The ICT industry, as the primary developer and provider of PETs, has a particularly important role to play with respect to the promotion of PETs. The Commission calls on all data controllers to more widely and intensely incorporate and apply PETs in their processes. For that purpose, the Commission will organise seminars with key actors of the ICT industry, and in particular PETs developers, with the aim of analyzing their possible contribution to promoting the use of PETs among data controllers.

The Commission will also conduct a study on the economic benefits of PETs and disseminate its results in order to encourage enterprises, in particular SMEs, to use them.

4.2.2. Action 2.2.: Ensuring respect for appropriate standards in the protection of personal data through PETs

While wide-reaching promotional activity requires the active involvement of the ICT industry, as the PETs producer, respect for appropriate standards requires action beyond selfregulation or the goodwill of the actors involved. The Commission will assess the need to develop standards regarding the lawful processing of personal data with PETs through appropriate impact assessments. On the basis of the outcome of such assessments, two sorts of instruments might be considered:

Action 2.2.a) Standardisation

The Commission will consider the need for respect of data protection rules to be taken into account in standardisation activities. The Commission will endeavour to take account of the input of the multi-stakeholder debate on PETs in preparing the corresponding Commission actions and the work of the European standardisation bodies. This will be paramount, in particular, where the debate identifies appropriate data protection standards requiring the incorporation and use of certain PETs.

The Commission may invite the European Standardisation Organisations (CEN, CENELEC, ETSI) to assess specific European needs, and to subsequently bring them to the international level by means of applying the current agreements between European and international standardisation organisations. Where appropriate, the ESOs should establish a specific standardisation work program covering European needs and thus complementing the ongoing work at international level.

Action 2.2.b) Coordination of national technical rules on security measures for data processing

National legislation adopted pursuant to the Data Protection Directive¹¹ gives national data protection authorities certain influence in determining precise technical requirements such as providing guidance for controllers, examining the systems put in place or issuing technical instructions. National data protection authorities could also require the incorporation and use of certain PETs where the processing of personal data involved makes them necessary. The

Commission considers that this is an area where coordination of national practice could contribute positively to promoting the use of PETs. In particular the Article 29 Working Party¹² could contribute in its role of considering the uniform application of national measures adopted under the Directive. The Commission thus calls on the Article 29 Working Party to continue its work in the field by including in its program a permanent activity of analyzing the needs for incorporating PETs in data processing operations as an effective means of ensuring respect for data protection rules. This work should then produce guidelines for data protection authorities to implement at national level through coordinated adoption of the appropriate instruments.

4.2.3. Action 2.3.: Promoting the use of PETs by public authorities

A consistent number of processing operations involving personal data are conducted by public authorities in the exercise of their competences, both at national and at Community level. Public bodies are themselves bound to respect fundamental rights, including the right to protect personal data, and ensure respect by others, and should therefore set a clear example. As regards national authorities, the Commission notes the proliferation of eGovernment applications as a tool for enhancing effectiveness of public service. As stated in the Commission's Communication on the Role of eGovernment for Europe's Future¹³, the use of PETs in eGovernment is necessary to provide trust and confidence to ensure its success. The Commission calls upon governments to ensure that data protection safeguards are embedded in eGovernment applications, including through the widest possible use of PETs in their design and implementation.

As for Community institutions and bodies, the Commission itself will ensure that it complies with the requirements of Regulation (EC) 45/2001 in particular through a wider use of PETs in the implementation of ICT applications involving the processing of personal data. At the same time, the Commission calls on other EU institutions to do the same. The European Data Protection Supervisor could contribute with his advice to Community institutions and bodies on drawing up internal rules relating to the processing of personal data. When selecting new ICT applications for its own use, or when developing existing applications, the Commission will consider the possibility of introducing privacy enhancing technologies. The importance of PETs will be reflected in the Commissions' overall IT governance strategy. The Commission will also continue to raise awareness in its own staff. However, the implementation of PETs in the Commissions' ICT applications depends on the availability of the corresponding products and will have to be evaluated on a case by case basis, in line with the application's development cycle.

4.3. Third objective: to encourage consumers to use PETs

Consumers will remain the most concerned party in ensuring personal information is properly used, that data protection rules are properly enacted, and that PETs are an efficient means to guarantee them.

Consumers should therefore be made fully aware of the advantages that the use of PETs may bring to diminish the risks posed by operations involving processing of their personal data. They should also be placed in a position where they may exercise an informed choice when purchasing IT equipment and software, or using e-services. This should reflect their awareness of the risks involved, in particular whether PETs offer appropriate protection. Simple and understandable information about possible technological tools to protect privacy must thus be provided to the user. Increased use of PETs and increased use of e-services which incorporate PETs will in turn mean economic reward to the industries using them, and may result in a snowball effect, encouraging other companies to pay greater attention to respecting the data protection rules. In order to achieve this, a series of steps should be taken.

4.3.1. Action 3.1.: Raising awareness of consumers

A consistent strategy should be adopted to raise consumer awareness of the risks involved in processing their data and of the solutions that PETs may provide as a complement to the existing systems of remedies contained in data protection legislation. The Commission intends to launch a series of EU-wide awareness-raising activities on PETs. The main responsibility for conducting this activity falls within the realm of national data protection authorities which already have relevant experience in this area. The Commission calls on them to increase their awareness-raising activities to include information on PETs through all possible means within their reach. The Commission also urges the Article 29 Working Party to coordinate national practice in a coherent work plan for awareness-raising on PETs and to serve as a meeting point for the sharing of good practice already in place at national level. In particular, consumer associations and other players such as the Consumer

Centres Network (ECC-Net), in its role as an EU-wide network to advise citizens on their rights as consumers, could become partners in the quest to educate consumers.

4.3.2. Action 3.2.: Facilitating consumers' informed choice: Privacy Seals

The take-up and use of PETs could be encouraged if the presence of these technologies in a certain product and its basic features are easily recognizable. For that purpose, the Commission intends to investigate the feasibility of an EU-wide system of privacy seals, which would also include an economic and societal impact analysis. The purpose of such privacy seals would be to ensure

consumers can easily identify a certain product as ensuring or enhancing data protection rules in the processing of data, in particular by incorporating appropriate PETs.

In order for privacy seals to achieve their purpose, the Commission considers that the following principles should be respected:

- The number of privacy seal systems should be kept to a minimum. In fact, a proliferation of seals may create more confusion to the consumer and undermine their trust in all seals. Therefore, an assessment should be made about whether and to what extent it would be appropriate to integrate a European privacy seal in a more general security certification scheme¹⁴

- Privacy seals should only be awarded for a product's compliance with a set of standards corresponding to data protection rules. The standards should be as uniform as possible throughout the EU.

- Public authorities, in particular national data protection authorities, should play an important role in the system through their involvement in the definition of relevant standards and procedures as well as in monitoring the functioning of the seal system.

With this in mind, and taking account of previous experience concerning seal programs in other areas (e.g. environment, agriculture, security certification for products and services), the ¹⁴In its Communication of 31 May 2006 on a Strategy for a secure Information Society “Dialogue, partnership and empowerment”(COM (2006) 251 final), the Commission has already invited the private sector to “work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy)”.

Commission will conduct a dialogue with all the stakeholders concerned, including national data protection authorities, industrial and consumer associations and standardisation bodies.

1.9 Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the processing of Personal Data.

Belgium

Status of legislative procedure

- Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data
- Modified by the implementation law of December 11, 1998 (O.J. 3.2.1999) [fr]
- Secondary legislation adopted on 13 February 2001 and published in the Official Journal of 13 March 2001.
- Entry into force: 01.09.2001 (exception for information when the data were not collected from the data subject then three years more).

Bulgaria

Status of legislative procedure

- Law for Protection of the Personal Data promulgated in the State Gazette 1/4 Jan 2002, in force as of 1 January 2002
- Amended in State Gazette, 70/10 August 2004, in to force as of 1 January 2005
- Amended in State Gazette 93/19 October 2004, amended in State Gazette 4/20 May 2005, in to force as of 1 September 2005
- Amended in State Gazette 103/ 23 December 2005, amended in State Gazette 30/11 April 2006, in to force as of 12 July 2006
- Amended in State Gazette 91/10 November 2006, amended in State Gazette 57/13 July 2007, in to force as of 13 July 2007

Czech Republic

- Consolidated version of the Personal Data Protection Act Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts

Denmark

Status of legislative procedure

- The Act on Processing of Personal Data (Act No. 429) of 31 May 2000
- Original version
- Entry into force: 01.07.2000.

Germany

Status of legislative procedure

The Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May

The Federal Data Protection Act applies to the federal publicsector and the private sector.

Entry into force: 23.05.2001.

All Länder (except Sachsen and Bremen) adopted new DPLs to implement the Directive. These acts apply to the public sector of the respective "Länder".

Baden-Württemberg

- Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz - LDSG) vom 27. Mai 1991, zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze vom 23. Mai 2000:

Bayern

- Bayerisches Datenschutzgesetz (BayDSG) vom 23. Juli 1993, zuletzt geändert durch Gesetz zur Änderung des Bayerischen Datenschutzgesetzes vom 25.10.2000 (Inkrafttreten zum 01.01.2001):

Berlin

- Berliner Datenschutzgesetz vom 17. Dezember 1990 (GVBl. 1991, S. 16, 54), geändert durch Gesetz vom 3. Juli 1995
- (GVBl. 1995, S. 404), zuletzt geändert durch Gesetz vom 30. Juli 2001 (GVBl. I, S. 66) (Inkrafttreten zum 5.8.2001)

Brandenburg

Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz - bgDSG) in der Fassung der Bekanntmachung vom 9. März 1999

Hamburg

Hamburger Datenschutzgesetz vom 5. Juli 1999, zuletzt geändert am 18. Juli 2001 (HmbGVBl. S. 216)

Hessen

Hessisches Datenschutzgesetz (HDSG) in der Fassung vom 7. Januar 1999

Mecklenburg-Vorpommern

Landesdatenschutzgesetz vom 28. März 2002 (GVOBl. M-V S. 154)

Niedersachsen

Niedersächsisches Datenschutzgesetz (NDSG) in der Fassung vom 29. Januar 2002 (Nds. GVBl. S. 22)

Nordrhein-Westfalen

Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen-DSG NRW-) idF. der Bekanntmachung vom 9. Juni 2000

Rheinland-Pfalz

Landesgesetz zur Änderung datenschutzrechtlicher Vorschriften vom 8. Mai 2002 (GVBl. S. 177)

Saarland

Gesetz Nr. 1477 zur Änderung des Saarländischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 22. August 2001 (Abl. S. 2066)

Sachsen-Anhalt

Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA)

Schleswig-Holstein

Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000

Estonia

Data Protection Act passed on 12 February 2003; entered into force on 1 October 2003 

Greece

Status of legislative procedure

Implementation Law 2472 on the Protection of individuals with regard to the processing of personal data

Original version

Entry into force: 10.04.1997

Spain

Status of legislative procedure

Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999).

Original version

Entry into force: 14.01.2000

France

Status of legislative procedure

Law 2004-801 modifying law 78-17 of 6.1.1978 ^[fr]

Ireland (*)

Status of legislative procedure

[Data Protection Act 1988](#)

Data Protection (Amendment) Act 2003 enacted on 10 April 2003

Entry into force on 1 July 2003

Italy

Status of legislative procedure

Protection of individuals and other subjects with regard to the processing of personal data
Act no. 675 of 31.12.1996


Entry into force: 08.05.1997

New Data Protection Code

Original Version

Entry into force: 01.01.2004

Luxembourg

DPL approved on 2 August 2002 and published in Memorial A 91 of 13 August 2002. 

Entry into force on 1 December 2002

Hungary

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

[Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest]

A Büntető Törvénykönyvről szóló 1978. évi IV. tv. 177/A és 177/B §-a (a visszaélés személyes adattal és a visszaélés közérdekű adattal büntetteinek tényállásai)

[Misuse of personal data, misuse of public information (Act IV of 1978 on the Criminal Code)]

Malta

Data Protection Act of December 14 200 (Act XXVI of 2001), as amended by Act XXXI of 2002
Full entry into force July 15, 2003

The Netherlands

Status of legislative procedure

DPL approved by the Senate on 06.07.2000 (O.J. 302/2000).
Original version:rotection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000

Entry into force on 1 September 2001.

Secondary legislation adopted

Austria

Status of legislative procedure

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 136/2001 of 17.08.1999 that applies to all processing by automatic

means.

Original version -

Entry into force: 01.01.2000.

Adopted ordinances: Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), Federal Law Gazette II Nr. 521/1999, about countries with adequate DP legislation (Switzerland and Hungary); Verordnung des Bundeskanzlers über das bei der Datenschutz- kommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2000 - DVRV), Federal Law Gazette II Nr. 520/1999, about the registration procedure; Verordnung des Bundeskanzlers über Standard- und Muster- anwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 - StMV), Federal Law Gazette II Nr. 201/2000, about exceptions from notification.

All nine Austrian Länder have adopted data protection laws to implement the Directive. These apply to processing otherwise than by automatic means.

Burgenland

Burgenländisches Datenschutzgesetz (Bgl. DSG), LGBl. Nr. 87/2005 (Inkrafttreten: 30.06.2005)

Kärnten

Kärtner Landesdatenschutz-Gesetz (K-LDSG), LGBl. Nr. 59/2000 (Inkrafttreten: 01.01.2000)

Niederösterreich

NÖ-Datenschutzgesetz (NÖ DSG), LGBl. 0901-1 (Inkrafttreten: 01.01.2001)

Oberösterreich

Gesetz vom 1. Juli 1988 über die Auskunftspflicht der Organe des Landes, der Gemeinden, der Gemeindeverbände und der durch Landesgesetz geregelten Selbstverwaltungskörper (oÖ.; Auskunftspflicht- und Datenschutzgesetz), LGBl. Nr. 46/1988; idF. LGBl. Nr. 41/2000

Salzburg

Gesetz über die Auskunftspflicht und den Datenschutz, LGBl. Nr. 73/1988, idF LGBl. Nr. 65/2001 (Inkrafttreten 01.07.2001)

Steiermark

Gesetz vom 20. März 2001 über den Schutz personenbezogener Daten in nicht automationsgestützt geführten Dateien (Steiermärkisches Datenschutzgesetz-StDSG), LGBl. Nr. 39/2001 (Inkrafttreten: 01.08.2001)

Tirol

Gesetz über den Schutz personenbezogener Daten (Tiroler Datenschutzgesetz - TDSG), LGBl. Nr. 60/2003 (Inkrafttreten: 21.05.2003)

Vorarlberg

Vorarlberger Landes-Datenschutzgesetz, LGBl. Nr. 19/2000 (Inkrafttreten: 01.01.2000)

Wien

Wiener Datenschutzgesetz (Wr. DSG), LGBl. Nr. 125/2001

Poland

Act of August 29, 1997 on the Protection of Personal Data, amended January 1, 2004, March 1, 2004, May 1, 2004

Cyprus

Νόμος που τροποποιεί τον Περι Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμο του 2001, αρ. 37(I)/2003

[The Processing of Personal Data (Protection of the Individual) Law of 2001, as amended in 2003]

Law of 2001

[Amendment (Law No. 37(I)/2003)]

Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, 112(I)/2004
[The Regulation of Electronic Communications and Postal Services Law of 2004 (112(I)/2004)]

Section 106 on unsolicited communications (spam)

Latvia

Fizisko personu datu aizsardzības likums

[Personal Data Protection Law Amended by Law of 24 October 2002]

Lithuania

Asmens duomenų teisinės apsaugos įstatymas (Law on Legal Protection of Personal Data) of 21 January 2003, No. IX-1296, With amendments of 13 April 2004 - Official translation

Portugal

Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecção de dados pessoais'

Entry into force: 27.10.1998

Romania

Status of legislative procedure

Law no. 677/2001 of 21st of November 2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data (published in the Official Journal of Romania, Part I No. 790 of the 12th of December 2001)

Law no. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing

Slovenia

March 1990: Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 9/1990; Entry into force: 24.03.1990)

July 1999: new Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 59/1999; Entry into force: 07.08.1999)

July 2001: Act Amending the Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 57/2001; Entry into force: 24.07.2001)

July 2004: new Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 86/2004; Entry into force: 01.01.2005) unofficial English Translation

December 2005: Information Commissioner Act (Published in Official Gazette of the Republic of Slovenia No. 113/2005; Entry into force: 31.12.2005) unofficial English Translation

Slovakia

Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll and the Act No. 90/2005 Coll.

Table of Compliance

Entry into force : 01/09/2002 (Act No 428/2002 Coll.)

01/12/2003 (Section 35 Paragraph 2)

01/01/2004 (Act No. 602/2003)

01/01/2005 (Act No. 576/2004)

01/05/2005 (Act No. 90/2005)

Finland

Status of legislative procedure

The Finnish Personal Data Act (523/1999) was given on 22.4.1999

Entry into force: 01.06.1999

Act on the amendment of the Finnish Personal Data Act

Entry into force: 01.12.2000

Finnish data protection act in working places

Entry into force : 01/10/2004

Sweden

Status of legislative procedure

Directive implemented by SFS 1998:204 of 29.4.98 and regulation SFS 1998:1191 of 03.09.98

Entry into force: 24.10.1998.

United Kingdom

Status of legislative procedure

Data Protection Act 1998 

Passed: 16.07.1998

Secondary legislation passed on 17.02.2000 [en](#)

Entry into force: 01.03. 2000.

EFTA States

Liechtenstein

Status of legislative procedure

Verordnung vom 9. Dezember 2008 über die Abänderung der Datenschutzverordnung

Gesetz vom 17. September 2008 über die Abänderung des Datenschutzgesetzes

Entry into force: 01.01.2009

Norway

Status of legislative procedure

LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven)
<http://lovdata.no/all/hl-20000414-031.html>, [Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act)]

Entry into force: 14.04.2000

1.10 Passenger Information Unit

Air carriers must transmit the PNR data ¹ in relation to international flights ², by electronic means, to specific bodies known as Passenger Information Units (PIUs). PIUs are designated by each Member State and are responsible for collecting the PNR data from the air carriers. The PIUs collect and analyse the data and carry out a risk assessment of the passengers. The purpose of this assessment is to identify the persons requiring further examination on the basis of the criteria provided for under national law. However, the competent authorities, like the PIUs, may not take enforcement action in relation to a passenger purely on the strength of automated processing of PNR data by the PIU and the competent authorities. These authorities, which are entitled to process the PNR data, are **designated by the States individually**. They consist solely of members of national services responsible for combating terrorism and organised crime.

In principle, these data are transmitted by the carriers 24 hours before the scheduled flight departure using the "push" method ³. Air carriers without databases established in a Member State of the European Union (EU) may either have recourse to the "push" method, or, if they do not possess the necessary technical architecture to use this method, permit the PIU to use the "pull" method ⁴. Air carriers may either transmit the data directly to the PIU or designate an intermediary for this purpose. In this case, this intermediary is responsible for collecting the data on behalf of the air carrier, centralising them in databases established only within EU territory, and then transmitting them to the PIU using the "push" method. In any case, air carriers inform passengers on international flights about the provision of PNR data. In the case of non-compliance with the rules laid down in the Framework Decision, Member States must provide for dissuasive, effective and proportionate sanctions against air carriers and intermediaries failing to transmit the PNR data. ⁵ These sanctions consist of:

- financial penalties in the case of transmission of incomplete or erroneous data;
- immobilisation, seizure or confiscation of the means of transport, or temporary suspension or withdrawal of the operating licence, in the event of serious, repeated infringements.

The PIUs of the various Member States exchange the PNR data contained in their respective databases. The competent authorities authorised by the Member States may also ask the PIU of another Member State to transmit such data to them. In exceptional circumstances, the PIU (or the competent authorities) may request the PIU of another Member State to provide PNR data prior to 24 hours before the scheduled flight departure. The transfer of data to the enforcement authorities of third countries is possible on condition that they are used for the purpose of fighting terrorism

and organised crime and that the receiving third country gives the Member State holding these data an assurance that it will not transfer them to another third country without the consent of that Member State. The data transmitted are governed by the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation. According to the proposal, these data, which must be necessary for the purposes of preventing and fighting terrorist offences and organised crime, are kept in a database for five years after their transfer to the PIU. The data may be kept for longer periods in cases where the person is the subject of an investigation of a terrorist offence or organised crime. Member States must comply with this Framework Decision by 31 December 2010. The Commission will evaluate the application of the instrument and 3 years after its entry into force will submit a report to the Council. Member States will provide the General Secretariat of the Council and the Commission with a list of PIUs, competent authorities, the text of the provisions transposing the Framework Decision and non-personal statistical information on PNR data transmitted by the air carriers to the PIUs.