COUNCIL OF THE EUROPEAN UNION

Brussels, 8 June 2004

9370/04

JURINFO 9

NOTE

from :	General Secretariat of the Council
to :	Working Party on Legal Data Processing
No. prev. doc. :	14455/03 JURINFO 19
Subject :	Right to anonymity in the sphere of Legal Data Processing

Delegations will find below the answers of delegations on the questionnaire set out in 14455/03 JURINFO 19. The answers are split up in the group of Member States who - in certain cases - protect the anonymity of judicial decisions that are published and an other group who generally do not protect them.

Protection of anonymity

No protection of anonymity

BELGIUM

The development of information and communication technologies offers significant opportunities and numerous benefits. However, use of these technologies also poses new threats to individual privacy and freedoms. Databases or files containing information relating to natural persons are created, used, transmitted and sold. As a result, the individual loses control over information which concerns him and the risk of abuse increases.

1. Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data

Since 1992 a Belgian law has guaranteed protection for individuals in regard to the use of their personal data. The law establishes a duty of transparency in relation to the use of personal data; those processing data must notify the persons who are the subject of the data, identify themselves and state the purpose of the processing. The law also lays down the rules governing the use of personal data: what may and must be done with the data collected. The law also stipulates that persons on file in data registers or databases are entitled to know what data is recorded about them, to have it corrected, and if necessary to oppose its distribution.

The data protected by the law is **personal data**.
Personal data means all information relating to an identified or identifiable natural person, whether they are Belgian or not. It might be the name of a person, a photograph, a telephone number (even a work telephone number), a code, a bank account number, an e-mail address, a fingerprint, etc. The concept is not confined to information about an individual's private life; it also covers information relating to professional or public life. However, the concept solely concerns information about natural persons: it does not cover information pertaining to legal persons (non-commercial partnerships, commercial companies, non-profit making organisations).

The law applies as soon as operations on personal data are performed - even if only partially - by **automatic means**, i.e. all information technologies: computers, telematics, telecommunication networks, the Internet, etc.
The law applies as soon as a single operation requires the involvement of automated means (e.g: the use of a fax to send a sheet of paper is subject to the law).
When operations on personal data are performed without the slightest use of automated means (particularly on paper or microfiche), the law must still be complied with if the data appears, or is intended to appear, in a manual file.

The law designates as the **data controller** the person (natural or legal), the "de facto" association or the public authority which determines the aims and means of the data processing. That person will be responsible if a problem arises. When the aims and means of processing are determined by a law, a decree or an order, the data controller is the person thus designated by the text in question.

The law does not apply when personal data is processed as part of activities which are exclusively personal or domestic, for instance an electronic personal diary.

Application of the law is partial in certain other cases, such as the processing of personal data solely for journalistic purposes or the purpose of artistic or literary expression. In such circumstances, it may happen that the provisions are not applied so as to ensure a balance with the protection of freedom of expression.

Processing carried out for the purposes of public safety also qualify for partial exceptions.

Data collection, whether direct or through the intermediary of a third party, must be carried out *fairly* i.e. by clearly and fully informing the persons who are the subject of the data collection. In principle, it is prohibited to gather "sensitive" data, i.e. data relating to race, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, criminal or administrative convictions. However, some exceptions are allowed (e.g. data required to administer medical care).

Data collection should have a *specific predetermined and legitimate aim*. There must be a **balance** between the interest of the data controller and the interests of the data subject.

Personal data may be processed only:

- if the data subject has unambiguously given his consent
- or if the data processing is required for the performance of a contract
- or if the processing is required by a law, decree or order
- or if the processing is necessary in order to protect a vital interest of the data subject
- or if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority
- or if the processing is necessary to pursue a legitimate interest on the part of the controller if the interest of the filer, in processing the data, is greater than the data subject's interest in the data not being processed.

The controller must **ensure** the quality of data, as well as the confidentiality, and security thereof. Personal data must not be kept in a form that will make it possible to identify the individuals concerned any longer than is necessary for achieving the desired objective. It should therefore be deleted or rendered anonymous.

Failure to meet these requirements exposes the infringer to a **fine** and, should the infringement be repeated, **imprisonment**.

The individuals concerned are **entitled to** *be informed*. They may question any controller to establish whether or not he holds any information on them. They are entitled *to receive a copy of the data being* processed as well as indication of the source of the data except in the case of data processed for reasons of State security, of public security and national defence, or for the prevention or prosecution of infringements where there is an indirect right of access via the Privacy Protection Commission.

Any party may have inaccurate data concerning him *rectified* free of charge and have incomplete, irrelevant or prohibited information *deleted or* have its use banned.

The **Privacy Protection Commission** receives complaints and takes action to ensure that the controller meets the obligations imposed by law. It endeavours to ensure that disputes are resolved amicably. Should it fail in this, it gives an opinion on whether the grounds for the complaint are sound. Should it establish that there has been an infringement of privacy, it will notify the public prosecutor accordingly. It may also bring the dispute before the President of the Court of First Instance.

2. Privacy and case-law database

Article 149 of the Constitution ordering that judgments be made public, is intended to protect citizens from arbitrary action by giving them access to the court hearing and the possibility of monitoring the reasoning on which the judgments are based. As a result of the wide dissemination of judicial judgments every citizen enjoys better access to the content of judgments and hence to the judges' interpretation of the regulations in force. It thus helps to ensure that everyone is better informed about legislation in force. Making judgments public also facilitates discussion of legal theory and critical comment. Informing all and sundry about the rights or wrongs of specific individuals is not therefore the objective .

The processing of personal data contained in a judgment delivered by a court is covered by the aforementioned **1992 Law on the protection of privacy with regard to the processing of personal data**. The protection of data concerns not only data relating to the parties but also data relating to judges or court officers, or data on third parties cited by the judgment.

*The **Privacy Protection Commission** initially considered reference to name only in court reports acceptable but since 1996 has found that automated searches in free text , available in CD Rom consultation software or on networks such as the Internet, make possible selection from extensive reports of judgments on the basis of the names of the parties combined with other search criteria. The technological advances which increase the possibilities for information searches must be accompanied by greater discretion when referring to data which can lead to identification of the parties in automated pages of caselaw and when searching other systems for the identification of legal judgments.*

The possibility of coming across someone's judicial record in centralised or exhaustive case-law databases poses risks to personal data protection out of all proportion to the risks attached to traditional modes of access or to the publication of case law.
The methods of consulting electronic data supports disseminating caselaw make it easy to abuse the caselaw data processing system through searches on the basis of the names of the parties or the names of the other persons involved in the dispute (experts, judges, lawyers, third parties cited).
The Commission adds that searches on the basis of the names of the parties or persons involved in the dispute should be banned.

Balance between the public's right to know (transparency) and individuals' right to protection of the data concerning them.

This balance may vary depending on different objective criteria linked to the nature of the dispute, the court in question and the categories of person concerned.

- the nature of the dispute:
  The names of the parties may be mentioned solely by their initials in the following cases: divorce, maintenance payments, minors, disciplinary matters , persons who are the subject of an internment order or before a review board, whenever mention of their name could be prejudicial to their legitimate interests. If the party's identity can be easily deduced, even by simple reference to initials, another reference will be used, for example, X, Y ou Z.
  The nature of certain cases automatically requires depersonalisation.

- the type of court:

Judgments of the Conseil d'Etat and the Court of Appeal are usually cited by reference to the names of the parties (ex: Marckx judgment).

- the person concerned:

  (a) third parties (witnesses and persons indirectly concerned by the case):
  there is absolutely no need to know their names or the nature of their contribution. Their names should not be mentioned in the judgment and there should be no possibility of carrying out searches on their names.

  (b) the persons involved in the dispute:
  the system for automatically rendering anonymous any data concerning the parties has yet to be finalised. In the meantime a right of consent could be established: when a lawsuit is filed the parties would be invited to indicate on an official form whether they consent to personal data concerning them being processed when the decisions are published electronically. In addition to the parties' refusal to have their names published, it should be possible for the courts to decide of their own accord to render decisions anonymous. A form clearly setting out the right of refusal and arrangements for exercising that right would be given to the parties as soon as a dispute is brought before the courts. In the case of absence of consent or of refusal, it would be obligatory for data to be depersonalised in every electronic publication of the decisions.

With regard to the **publication** of disputes **on paper**, the Commission does not consider depersonalisation necessary, except in cases in which it is legally required.

As far as the names of magistrates, experts and lawyers and court officials in general are concerned, the Commission emphasises that the general public's right to know the identity of the persons who delivered a decision and of those who worked on it carries the more weight. Under certain circumstances, court officials who do not wish to have their names associated with a specific case would have the right to depersonalisation by filling in a form.

It ought to be possible to exercise the right to depersonalisation free of charge through simple procedures, not only when the lawsuit is filed but also after the decision has been delivered, vis-à-vis the publisher.

The law of 11 December 1998 transposing 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 has fully replaced **Article 8 of the 1992 law** on the protection of privacy with regard to the processing of personal data. That Article now reads as follows:

"1.The processing of personal data regarding disputes brought before the lawcourts, tribunals and administrative courts, regarding suspicions, prosecutions or sentences relating to offences, or regarding administrative penalties or preventive measures is prohibited.

2. The ban on the processing of the personal data referred to in paragraph 1 shall not apply to processing carried out:

(a) under the control of a public authority or of a ministerial officer within the meaning of the Judicial Code, where such processing is necessary for the performance of their duties;

(b) by other persons where such processing is necessary to achieve purposes determined by or by virtue of a law, decree or order;

(c) by natural or legal persons of public or private law if required for the conduct of their own litigation;

(d) by lawyers or other counsels of the court if required for the defence of their clients;

(e) for the needs of scientific research, subject to the conditions determined by the King by means of a decree discussed in the Council of Ministers, after obtaining the opinion of the Privacy Commission;

3. Persons who, by virtue of paragraph 2, are authorised to process the personal data referred to in paragraph 1, shall be subject to professional secrecy.
4. The King shall determine, by means of a decree discussed in the Council of Ministers, after obtaining the opinion of the Privacy Commission, the special conditions which must be met by the processing of the personal data referred to in paragraph 1."

Article 8(2)(e) thus allows judicial personal data to be processed for scientific purposes, subject to certain conditions.

A Royal Decree of 13 February 2001 implementing the law of 8 December 1992 on the protection of privacy with regard to the processing of personal data put the finishing touches to the amendments made by the 1998 law. It sets the date for the entry into force of the 1998 law and it alone replaces more than ten previous implementing decrees.

Accordingly, depersonalisation is the rule for judicial personal data in databases unless its scientific nature can be established.

3. Privacy and legislative databases

The fact that personal data must be publicly disseminated so that the legal effects can be relied on as against third parties does not prevent the application of the 1992 law on the protection of privacy with regard to the processing of personal data, since the 1998 amendment. Respect for the principles of finality and proportionality with regard to data of this kind must therefore also be examined.

The purpose of publishing such personal data is indisputably legitimate. However, respect for the principle of proportionality requires that personal data published in this manner must be adequate, relevant and not excessive.

The Commission recommends that users' attention be drawn to the provisions of the 1992 law on the protection of privacy with regard to the processing of personal data. A notice should remind users that the collection of personal data without the consent of the data subject and their use for purposes other than those for which they were gathered is liable to a fine and, in the event of a repeat offence, imprisonment. The judge may also order the confiscation of the data carrier or the deletion of the data.

4. Post-processing for Historical, Scientific or Statistical purposes (HSS)

The general principle is that post-processing of personal data for HSS purposes must be performed using anonymous data, in other words, data which do not enable the data subject to be reidentified by a third party.

If the HSS purposes cannot be achieved using anonymous data, the data controller responsible for the post-processing may use coded data, i.e. personal data not including data for direct identification.

If the HSS purposes cannot be achieved using this working method, the data controller responsible for the post-processing may use non-coded data.

The post-processing of anonymous data does not have to be declared in advance to the Commission, as the data is no longer personal.

The Commission must be informed of the post-processing of personal data, codified or non-codified, using ad hoc forms within a given deadline.

5. References

1. Legal provisions

Type of text	Date of issue	Publication in the *Moniteur Belge*		File number in the *Legislation consolidée* on http://www.just.fgov.be
		Date	Page	
Law	8.12.1992	18.3.1993	5 801	1992-12-08/32
Law	11.12.1998	3.2.1999	3 049	1998-12-11/54
Royal Decree	13.2.2001	13.3.2001	7 839	2001-02-13/32

2. Opinions of the Privacy Commission[1]

Internet site: http://www.privacy.fgov.be (Jurisprudence on http://www.just.fgov.be)
E-mail. commission@privacy.fgov.be

CZECH REPUBLIC

Does the Czech Republic protect or not the anonymity of judicial decisions that are published?

According to the Act No. 182/1993 Coll. on the Constitutional Court and to the Act No. 309/1999 Coll. on the Collection of Acts and the Collection of International Treaties **decisions of the Constitutional Court of the Czech Republic** shall be published in the Collection of Acts.
Furthermore decisions of the Constitutional Court shall be published in the Collection of Judgments and Rulings of the Constitutional Court issued by the Constitutional Court.
Decisions adopted by the Constitutional Court are available on the Internet.

[1] The opinions on which this summary document are based are available on these Internet sites.

The Supreme Court of the Czech Republic issues the Collection of courts decisions and positions. Decisions adopted by the Supreme Court are available on the Internet.

Decisions of **the Supreme Administrative Court of the Czech Republic** are published in the Collection of decisions of the Supreme Administrative Court. The Internet site on which the decisions shall be available is being in preparation.

The right to anonymity in connection with published decisions mentioned above is protected, personal data are covered, and only first letters of names (initials) are used.

Can the unauthorized or prohibited publication of identifiable references lead to criminal or civil liability?

- Protection according to the Civil Code

Civil liability appears suitable with reference to the factual res gestae. It may be either civil liability according to the ***Article 16 of the Civil Code*** *(general clause), which states:* „person who causes damage by an unauthorised interference with the right to protection of personality shall be responsible for the damage in accordance with the adequate provision of this Statute constituting liability for damage“ *or civil liability according to the* ***Article 13 of the Civil Code*** *(special protection) which states:* „natural person has right to claim that others refrain from unauthorised interference with her right to protection of personality, right to remedy of consequences of such interference and right to appropriate compensation.“

- Protection according to the Criminal Code

Provision of the ***Article 206 of the Criminal Code*** *may apply when considering the criminal protection. It stipulates:* „person who about another imparts false statement capable of jeopardizing his personal respect by means of disadvantaging him at work, impairing his family relations or causing other serious harm, shall be punished with the imprisonment for up to one year.“

Another example to think of is the criminal act of exposure of classified information *according to the* ***Article 106 of the Criminal Code****:* „Who searches for classified information (classified in the meaning of special act) with the purpose of revealing it to an unauthorised person, who for such purpose collects data containing classified information, or who deliberately discloses the classified information to an unauthorised person…" *Further shell be reflected the* criminal act of infringing others´ rights *according to the* ***Article 209 of the Criminal Code****. Res gestae is met by one who causes serious detriment to rights of another person by misleading such person or taking advantage of that person's mistake.*

- protection according to the Act on the Protection of Personal Data

According to the **Article 4** of **the Act on the Protection of Personal Data** the *personal data* shall mean any data relating to an identified or identifiable data subject. *A data subject* shall be considered to be identified or identifiable if his/her identity can be directly or indirectly determined on the basis of one or more items of personal data. Data shall not be considered personal data where inadequate quantity of time, effort or material resources are required to determine the identity of the data subject.

According to the ***Article 10*** *in personal data processing, the controller and processor shall ensure that the rights of the data subject are not infringed upon, in particular, the right to preservation of human dignity, and shall also ensure that the private and personal life of the data subject is protected against unauthorized intervention.*

Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity be amended?

Under the **Articles 156 and 157** of the **Act No 99/1963 Coll., Civil Procedure Code**, and under the **Article 200** of the **Act No 141/1963 Coll., Criminal Procedure Code**, *a judgment is always announced publicly*. In the civil procedure it is announced by the president of the senate in the name of the Czech Republic and contains the name of court, the full names of judges and attending judges, exact identification of participants and their representatives. If possible, the identification of participants includes also their dates of birth (identification numbers).

In the criminal procedure the judgment contains the full name, date of birth, place of birth, place of residence and other information eligible for identification of the defendant.

The restriction *is based on the **Act No. 101/2000 Coll., on Protection of the Personal Data** and on Amendments to Some Related Acts. Under the **Article 11** the controller shall not be obligated to provide the information under subsection if the controller is processing the personal data exclusively for statistical, scientific or archival purposes; if the law stipulates the obligation of the controller to process the personal data; and if a specific Act stipulates that the controller is not obligated to provide the personal data.*

In connection with the facts mentioned above it is suitable to point out the institute of concealed witness *under the **Article 55** of the **Act No. 41/1961 Coll., Code of Criminal Procedure**. If the circumstances indicate that the concealed witness or the person in near relationship with the concealed witness are jeopardized by bodily injury or other serious danger of infringement of their fundamental rights in the connection with the concealed witness' evidence, and if there is no other way to protect the concealed witness reliably, the competent authorities apply provisions to conceal the identity and the portrait of the concealed witness, full name and other personal data of the concealed witness aren't filled in the record.*

They are filled separately and are underlain only to competent authorities. If all of the appropriate presumptions are satisfied, the judgment doesn't contain the personal data of the concealed witness. In the other case it is possible to demand to put this data out of the record.

In the case of databases, is there a procedure for the automatic suppression of personal data?

In accordance with the ***Article 11 (5)*** *of* ***the Act No. 101/2000 Coll. on Protection of the Personal Data and on Amendments to Some Related Acts*** *the controller may provide information without acceptance of the data subject if he is processing personal data exclusively for statistical, scientific or archival purposes.*

In personal data processing, the controller and processor shall ensure that the rights of the data subject are not infringed upon, in particular, the right to preservation of human dignity, and shall also ensure that the private and personal life of the data subject is protected against unauthorized intervention (Article 10).

Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?

In accordance with the **Article 5** of **the Act No. 101/2000 Coll. on Protection of the Personal Data and on Amendments to Some Related Acts** the controller shall be obliged to process only authentic and accurate personal data, which he obtained in conformity with this Act. The controller shall be obligated to verify whether the personal data are authentic and accurate. If the controller finds that the data that are being processed thereby are not authentic or accurate with respect to the specified purpose, in particular, in relation to an objection raised by the data subject, the controller must block the personal data and correct or supplement them without undue delay. If the data cannot be corrected or supplemented, the controller must liquidate them without undue delay. Inauthentic, inaccurate, or unverified personal data may be processed only in cases stipulated by a special Act. These data must be duly designated and kept separately from other personal data

In personal data processing, the controller and processor shall ensure that the rights of the data subject are not infringed upon, in particular, the right to preservation of human dignity, and shall also ensure that the private and personal life of the data subject is protected against unauthorized intervention.

Regarding the civil protection the person who assumes to be involved by these facts may ask court to issue a precaution according to the Civil Procedure Act (99/1963 Coll., as amended). (See answer to the first question as well)

GERMANY

The German Federal Government agrees in principle with the thinking of the Italian delegation. The right of persons involved in legal proceedings to protection of their personal data is in conflict with the interest of the general public and experts in being informed. It must therefore be decided which interest should take precedence. It must also be borne in mind that modern information technology offers new and appreciably greater opportunities for disseminating, searching for and linking information. This can have a substantial impact on the lives of those concerned.

I. Current practice as regards publication of court decisions

To facilitate understanding of the legal framework and the replies to the individual questions, we will first briefly describe current practice as regards publication of court decisions in Germany.

As a rule, court decisions are published by private publishing companies in journals and databases. The Federal Constitutional Court, the highest Federal Courts and the higher Courts of the Länder (including the Higher Regional Courts [Oberlandesgerichte] and the Higher Administrative Courts [Oberverwaltungsgerichte]) also publish collections of their own decisions in print and on their Internet websites.

All types of publication serve in the first place to keep legal experts informed. Regardless of the legal obligation to make them anonymous, decisions are therefore mostly published only in a very abridged form; in particular, the names and addresses of the parties and their lawyers which, under German procedural law, are summarised at the beginning of a decision (so-called "rubric"), are omitted or abbreviated.

As a rule, simply leaving out the rubric has the effect of making decisions anonymous, since elsewhere in the text the parties are mentioned only by reference to their respective roles (e.g. plaintiff or defendant) and it is usually not possible to establish the identity of a person not party to the proceedings. Where the findings and the grounds for the decision contain personal data (e.g. names of witnesses) or other details that enable a person's identity to be established, these too are made anonymous.

All published court decisions originate in the registries of the courts, to which each judge is assigned. One of the tasks of the registries is to send out court decisions on request to private individuals or publishers in the prescribed form.

II. Legal framework

1. Principle: only anonymous publication

In Germany there is no general legislation governing the publication of court decisions; the question of making them anonymous is therefore not explicitly regulated by law. However, it is a long tradition that decisions are, in principle, only published in an anonymous form. Today this is also a consequence of Federal and Länder data protection laws, which are based on EU Directive 95/46/EC.

This principle is also set down in the registries' administrative rules although these have no legal force: they are simply internal administrative instructions. The courts must abide by the principle whether any party to a case so requests or not.

2. Exceptions

In certain cases, e.g. convictions for defamation or unfair competition, the law prescribes that the court shall make its decision public on application by the injured party. In this case, publication includes all details relating to the person convicted. The reason for these exceptions is to enable the injured party to inform the general public in a simple fashion about the breach of the law committed by the person convicted.

These provisions constitute authority to communicate personal data within the meaning of data protection law.

III. Replies to the individual questions

Question 1:
Decisions may in principle only be published in an anonymous form (see II. above).

Question 2:
As decisions may only be published in an anonymous form, the courts must make them anonymous on their own initiative (see II. above).

Question 3:
The purpose of the anonymity obligation is to uphold the right of the persons involved to protection of their private life.

Question 4:
The balance between the interests of a person affected and the general public is reflected in the principle and the exceptions to it, as described under II.

Question 5:
The anonymity obligation also applies to publication in specialist journals. However, as indicated in I., this does not pose any practical problem, since such journals are not interested in publishing personal data anyway.

Question 6:
No. The anonymity obligation applies to all forms of publication in the same way.

Question 7:
The use of personal data, i.e. including court decisions that have not been made anonymous, for research purposes is governed by general data protection law and - as regards research in the area of criminal law - by the Code of Criminal Procedure. The relevant provisions lay down that data may only be communicated insofar as necessary for the purpose of the research and where public interest in the project outweighs the interest of the person involved in maintaining confidentiality.

The personal data communicated may be used only for the specific research project and must be made anonymous as soon as the purpose of the research allows. The researchers involved must keep the data confidential.

Question 8:
Unlawful publication of decisions that have not been made anonymous constitutes unauthorised communication of personal data. This is an administrative offence and may be punished with a fine. Under certain conditions it may also be prosecuted as a criminal offence.

Civil liability is possible under the provisions of data protection law and the general rules regarding the liability of state bodies for illegal acts.

Question 9:
A right to have data corrected and to have court decisions that have already been published made anonymous subsequently exists under the general data protection law. Where a decision is made anonymous subsequently, this constitutes deletion of data.

Question 10:
As described under I., one of the registries' tasks is to send out decisions only in the prescribed form, i.e. usually in an anonymous form. Personal details are already removed at that stage and there is therefore no publicly accessible legal database containing decisions which include personal details.

The process of making decisions anonymous is carried out manually. Software tools are now being developed to automate this process.

Question 11:
Intervention by state authorities is possible under data protection law. However, the powers of the supervisory authorities are limited. The authorities can lodge a complaint with public bodies about unlawful publication and also inform the authorities responsible for prosecuting criminal or administrative offences.

GREECE

Our replies to the questionnaire from the Italian Presidency in document 14455/03 JURINFO 19 of 7 November 2003, concerning the right to anonymity in the context of legal data processing, are set out below.

With reference to the first section of the questionnaire, relating to the application of principles to protect privacy:

Introduction

- The legislative framework in Greece for protecting individuals with regard to the processing of personal data is provided by Law 2472/1997, which came into force on 10 April 1997. By means of that Law, Greece complies with the principles of the Community Directive of 24 October 1995.

- The Law establishes an independent authority to protect personal data, with the task of supervising application of the Law in question and of other provisions relating to the protection of individuals with regard to the processing of personal data.

– On the basis of Article 7 of Law 2472/1997, the Hellenic Data Protection Authority grants permits for the establishment of files containing sensitive data, such as the texts of court decisions which may contain personal data relating to social security, criminal proceedings and charges.

  Under the terms of the permit, the recording of such decisions in a legal database is allowed provided that the parties to the case and other natural persons involved are first rendered anonymous. An exception from anonymity is made for the lawyers arguing the case and for the natural persons constituting the court.

– Anonymity applies in every case, whether or not the person concerned has requested it, in accordance with the permit to establish the file; in addition, under Articles 11 to 14 of Law 2472/97, the data subject has the right to be informed, to have access, to object and to obtain provisional judicial protection.

– Under Article 1 of Law 2472/1997, the purpose of eliminating data which could identify individuals is to protect the rights and fundamental freedoms of natural persons and in particular the privacy of data subjects.

– The right to information must not extend any further than necessary. That is to say that an individual's privacy must not be infringed by any publication referring to him.

  Preserving anonymity enables specialised legal information to be made directly available while at the same time ensuring that use of the content of decisions does not disclose the personal data of the data subject.

– Yes, anonymity applies in these cases too. When judicial decisions are published in legal reviews or in the press, only the parties' initials are given, but even that practice is tending to disappear.

  Publishers and specialists working for legal reviews remove data which could identify natural persons, and have been doing so since well before the adoption and entry into force of Law 2472/1997 (it is a characteristic of our legal culture that, since 1945, the anonymity of the parties involved in judicial decisions has been preserved).

  Some legal reviews avoid giving even the initials. Instead, they insert an asterisk or simply refer only to the legal identity of the parties (e.g. the accused, civil party to the proceedings etc.).

– The same level of legal protection applies to both publication on the Internet and publication in print.
  Because of the limitations of printed material, legal reviews in principle have a limited capacity for publishing decisions.

  Databases on the Internet, on the other hand, in theory have unlimited capacity.

  Consequently, protection levels with regard to databases offer more technical possibilities.

– Under Article 7(2)(f) of Law 2472/1997, data may be processed only for research and scientific purposes and provided that anonymity is maintained and all necessary measures for the protection of the persons involved are taken.

With reference to the second part of the questionnaire, concerning the legal framework which imposes restrictions on the processing of data:

- Yes, there are rules governing such cases and imposing restrictions on the use which may be made of data by those processing it.

– Articles 21 to 23 of Law 2472/1997 provide for administrative and criminal penalties and civil liability should those responsible for processing personal data fail to fulfil their obligations.

– Under Articles 13 and 14 of Law 2472/1997 data subjects are entitled to object at any time to the processing of data relating to them and all data subjects have the right to apply to the competent court for the immediate suspension or non-application of acts or decisions affecting them which have been issued by an administrative authority or public law entity or private law entity or association or natural person solely by means of automated processing of data, when such processing is intended to assess their personality and especially their effectiveness at work, creditworthiness, reliability and general conduct.

– We are not acquainted with the mechanisms and technical possibilities of all databases. In the specific case of the Athens Bar Association's databases there is a procedure preventing searches based on the names of natural persons (in technical terms, a "stopword list" is created which blocks searches based on the names of natural persons).

– Anyone who unlawfully interferes in any way with a file containing personal data or accesses such data or extracts, alters, damages, destroys, processes, transfers or discloses such data or makes them accessible to unauthorised persons or permits such persons to have knowledge of them, or exploits them in any way is liable to criminal penalties and incurs civil liability under Articles 22 and 23 of Law 2472/1997. Under Article 21 of that Law, the Authority imposes administrative penalties on data controllers or their representatives if they are found to be in breach of their duties under the Law in question or under any other regulation relating to the protection of individuals with regard to the processing of personal data; these penalties may consist of a warning with a deadline for cessation of the breach, temporary or definitive revocation of permit, destruction of the file or a ban on processing and destruction of the relevant data.

SPAIN

- **To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?**

Under Regulation No 5/1995 of the High Council of the Judiciary of 7 June 1995 on ancillary aspects of judicial proceedings, as amended by the High Council's Decision of 18 June 1997 (Spanish official gazette of 2 July 1997), "in the processing and dissemination of judicial rulings, every effort shall be made to remove identity details, so as to protect personal and family reputation and privacy at all times".

- **Are they eliminated in every case or only at the request of the person concerned?**

In all cases.

- **For what purposes do the rules impose the removal of references that would make identification possible?**

For the protection of personal and family privacy.

- **Is the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation accepted? To what extent?**

This is not a principle recognised by Law No 15/1999 of 15 December 1999 on protection of personal data. However, there is a well-developed, consistent body of Constitutional Court case law recognising the need for such a balance and establishing it.

- **Legal data are often published in periodicals intended for the general public or in publications for lawyers and other members of the legal profession. Is the anonymity criterion applied in such cases too?**

As a rule, yes.
In the case of minors, naming them is expressly prohibited by Framework Law No 1/1996 on legal protection of minors.

- **Do different levels of protection exist for publication on the Internet and in print?**

No. Publication of personal data on the Internet is basically subject to the same general rules and requirements as for disclosure of data by any other means, under Article 11 of the Law on protection of personal data.

- **Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes. Are there rules governing such cases, which impose restrictions on their use or discretion on those who process the data or on researchers?**

Yes, Law No 12/1989 of 9 May 1989 on public statistics.
In addition, under Article 11(2) of the Law on protection of personal data, the data subject's consent is not required for disclosure of personal data "where data are supplied by one public administrative authority to another, for subsequent processing for historical, statistical or scientific purposes".

- **Can the unauthorised or prohibited publication of identifiable references lead to criminal or civil liability?**

Yes. In the case of a public database, a liability claim will be pursued under the legislation governing liability on the part of public authorities. In the case of a private database, a liability claim will be pursued in the ordinary courts.

Article 197 of the Penal Code makes such disclosure a criminal offence.

- **Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity be amended?**

Criminal procedure does not recognise any right to anonymity. As a rule, judicial proceedings are made public. Under Spanish law, there is no general principle of anonymity, nor is it a procedural right. The one purpose for which anonymity has been introduced is the processing and dissemination of judicial rulings.

It is possible for the courts to order that witnesses and experts remain anonymous, i.e. that their identity not be shown in the records of a case, under Framework Law No 19/1994 of 23 December 1994 on protection of witnesses and experts in criminal proceedings, but this does not apply to defendants.

- **In the case of databases, is there a procedure for the automatic suppression of personal data?**

No.

- **Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?**

The courts can take action, upon application by a data subject, to have information corrected, should a media organisation disregard the data subject's request for correction.

HUNGARY

To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?

There are no specific legal provisions for the publication of judicial decisions in Hungarian law; Act LXIII of 1992 on the protection of personal data and on the publicity of public interest information (the Data Protection Act) applies to these publications as well. Consequently, there are in principle no names or identifiable references in the published version of judicial decisions. Parties or other participants in judicial proceedings are traditionally referred to by their position in the proceedings (plaintiff, defendant, etc.) or by initials.

Are they eliminated in every case or only at the request of the person concerned?

They are eliminated without request.

For what purposes do the rules impose the removal of references that would make identification possible?

The rules that impose the removal of references that would make identification possible are the rules protecting personal data. The protection of personal data is enshrined in Art. 59 of the Constitution.

Is the principle of a fair balance between the citizens' right to information and the right of the person named to defend their reputation accepted? To what extent?

The Hungarian legal system does not recognise a general right of the public to obtain information on the identity of parties involved in judicial or administrative proceedings. This principle is however not without exceptions.

The most important exception is when the court case involves issues of important public interest, eg. proceedings in which public figures are parties because of reasons connected to their public function. In this case the citizens' interest in obtaining information on the case can be deemed to be stronger that the individual interest of the parties and, as a consequence, there have been examples of the publication of judicial decisions containing personal data.

Another case of court decisions being published together with the personal data contained therein is where the publication itself is a sanction of some unlawful act, eg. in defamation or unfair competition cases.

Legal data is often published in periodicals intended for the general public or in publications for lawyers and other members of the legal profession. Is the anonymity criterion applied in such cases too?

Yes. The same principles and legal framework apply to publications for members of the legal profession than to any other publications.

Do different levels of protection exist for publication on the internet and in print?

No. The same principles and legal framework apply to publications on the internet and in print.

Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes. Are there rules governing such cases, which impose restrictions on their use or discretion on those who process data or on researchers?

Yes. Article 32 of the Data Protection Act applies to scientific research and article 32/A of the Data Protection Act to statistics. These provisions restrict the use of personal data collected for these specific purposes to these purposes only. In case of data collected for research, they must be made anonymous as soon as the purpose of the research allows. Personal data collected for research purposes may be published if this is necessary to present the results of research on historical events.

Can the unauthorised or prohibited publication of identifiable references lead to criminal or civil liability?

Yes. Art. 18 of the Data Protection Act provides for the rules on civil liability and Art. 177-177/A of the Penal Code for the rules on criminal liability.

Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity be amended?

Yes. The right to have the consequences of unlawful data processing set aside exists under general data protection law. This means the right to have incorrect data corrected and to have unlawful references infringing anonymity deleted.

In the case of databases, is there a procedure for the automatic suppression of personal data?

Since published judicial decisions, as a main rule, do not contain personal data, there are no public databases containing such data. As for court databases, there exists no procedure for the automatic suppression of personal data.

Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?

Yes. Protection is provided for by general data protection law.

THE NETHERLANDS

To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?

See EC Directive 95/46 of 24 October 1995. In the Netherlands, the provisions of the Directive are incorporated in the Personal Data Protection Act. While this Act does not contain any specific provisions on disidentification, it prohibits the processing of personal data where the interests of privacy prevail. Particular personal data, such as details of a criminal record, may not generally be processed, subject to exceptions specified in the Act. To prevent the need for constant assessment, established policy is that all legal rulings are disidentified upon publication.

Are they eliminated in every case or only at the request of the person concerned?

See the reply to the previous question.

For what purposes do the rules impose the removal of references that would make identification possible?

See the reply to the first question.

Is the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation accepted? To what extent?

Yes. This principle is laid down in the Code of Civil Procedure, the General Administrative Law Act and the Penal Code.

Article 8:79, second paragraph, General Administrative Law Act: Persons other than parties may obtain copies of or extracts from the judgment or the record of the oral judgment. (Note: respect for privacy require that in certain circumstances only an extract may be issued.)

Article 28, paragraph 2, Code of Civil Procedure: (The clerk of the court) shall issue to anyone who so requires copies of orders, rulings or decisions, unless the clerk of the court considers that he should refuse such issue in part or entirely to protect important interests of others, including those of the parties. In the latter case, the clerk may only issue a disidentified copy of or extract from the order, ruling or decision.

Article 28, paragraph 3, Code of Civil Procedure: orders, rulings or decisions shall be understood to mean documents attached to the judgment. No copies of or extracts from other documents making up the case file shall be issued.

Article 28, paragraph 4, Code of Civil Procedure : In the case of orders, rulings and decisions in matters dealt with in camera, only a disidentified copy or extract shall be issued.

(Since the entry into force of the bill on judicial and criminal data) Article 365, fourth paragraph, of the Code of Criminal Procedure reads as follows: If requested, the president shall issue an extract from the sentence and the record to all persons other than the suspect or his counsel unless he considers that such issue should be refused in part or entirely to protect the interests of the person who is the subject of the sentence or of third parties named in the sentence or record. In the latter case, the president may issue a disidentified copy of or an extract from the sentence and the record.

Article 365, fifth paragraph of the Code of Criminal Procedure then reads: The sentence shall be understood as documents attached to the judgement.

No copies of or extracts from other documents making up the criminal file shall be issued.

Legal data is often published in periodicals intended for the general public or in publications for lawyers and other members of the legal profession. Is the anonymity criterion applied in such cases too?

No specific legal rules exist on the provision of information by courts to publishers of newspapers and (legal) periodicals. What publishers do with information they obtain from parties, lawyers or other persons with knowledge of personal data is their own responsibility.

Do different levels of protection exist for publication on the internet and in print?

No.

Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes. Are there rules governing such cases, which impose restrictions on their use or discretion on those who process the data or on researchers?

Yes. The Personal Data Protection Act provides that the data controller is to take the necessary steps to ensure that additional processing is carried out solely for these specific purposes. As regards particular data, processing should also include safeguards to ensure that the privacy of the persons concerned is not disproportionately infringed.

Can the unauthorised or prohibited publication of identifiable references lead to criminal or civil liability?

Yes. The Personal Data Protection Board (established by the Personal Data Protection Act) may impose a fine if the Personal Data Protection Act is violated. In addition, violations of privacy law generally entail civil liability.

Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity be amended?

Yes. In the context of civil liability, the injured party may demand that anyone who has unlawfully invaded his right to privacy be ordered to take measures to put an end to the illegality. (Naturally, the actual substance of legal rulings may be challenged solely using the appropriate legal means - an appeal to a higher court, the court of cassation or similar.)

In the case of databases, is there a procedure for the automatic suppression of personal data?

No, although there are guidelines on disidentification for the transmission of rulings to the database administrator.

Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?

Pursuant to the Personal Data Protection Act, the Personal Data Protection Board may take quite far-reaching measures, including coercive administrative measures. Those concerned can always ask the Personal Data Protection Board to take steps against the controller on that basis but this does not constitute a specific measure in the interests of the particular parties concerned.

AUSTRIA

– *To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?*

Under the relevant provisions annexed to this note (§§ 15 and 15a of the Supreme Court Act, § 48a of the Organisation of the Courts Act) names, addresses and, where necessary, place names in the *Entscheidungsdokumentation Justiz* (case-law database), which is generally accessible via the Internet, or in printouts from that database, which allow inferences to be drawn regarding the case concerned must be rendered anonymous by the use of letters, numbers or abbreviations, without impeding the intelligibility of the decision. In cases in which the proceedings were conducted without a public hearing at all instances, the courts may also order that the decision (full text) is not to be published in the database if the anonymity of those concerned cannot otherwise be guaranteed. It should be emphasised that decisions relating to anonymity and publication are taken by the courts.

– *Are they eliminated in every case or only at the request of the person concerned?*

They are always eliminated, whether or not an individual request is made.

– *For what purposes do the rules impose the removal of references that would make identification possible?*

To protect the privacy of the parties to proceedings.

– *Is the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation accepted? To what extent?*

The Austrian legal system does not recognise any general interest in obtaining information on court cases **including the identity of the parties to the proceedings**. In individual cases it is possible to obtain information on certain proceedings in addition to the published text of court rulings through the procedure for consulting official documents. The decision on whether to grant permission to consult official documents in accordance with the Code of Civil Procedure or the Code of Criminal Procedure (in particular § 219 of the Code of Civil Procedure and § 82 of the Code of Criminal Procedure) falls within the jurisdiction of the independent courts. The provisions on anonymity and publication of court rulings endeavour to strike a balance between protecting the privacy of the parties to proceedings and the intelligibility of court rulings. In trademark disputes, for instance, the trademark is not kept anonymous in order to enhance the intelligibility of the decision.

– *Legal data is often published in periodicals intended for the general public or in publications for lawyers and other members of the legal profession. Is the anonymity criterion applied in such cases too?*

Yes.

– *Do different levels of protection exist for publication on the Internet and in print?*

No.

– *Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes. Are there rules governing such cases, which impose restrictions on their use or discretion on those who process the data or on researchers?*

Apart from the restrictions on the publication of rulings or printouts already mentioned, Article 20(3) of the Austrian Federal Constitution stipulates that, unless otherwise provided by law, all officials entrusted with administrative duties relating to the Federation, the States or the districts and officials of other public-law bodies are under an obligation of discretion concerning all facts which come to their knowledge exclusively through their official activity and the confidentiality of which is necessary in the interest of maintaining public peace, order and security, of general national defence or of foreign relations, or in the economic interest of a public-law body, or for the preparation of a ruling, or **in the overriding interest of the parties concerned.**
(official secrecy)

A breach of this obligation of discretion is liable to punishment as an offence pursuant to § 310 of the Penal Code.

As far as statistics in the Federal legal information system are concerned, no personal data are evaluated and statistics are only kept on the number of documents and user queries.

– *Can the unauthorised or prohibited publication of identifiable references lead to criminal or civil liability?*

In addition to the provision of § 310 of the Penal Code, consequences under criminal law could also ensue pursuant to § 113 of the Penal Code (accusation of an offence punishable by the courts when the case is closed). Depending on the circumstances of the case, such publication could also have legal consequences under civil law.

The general rules on official liability also apply.

– *Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity by amended?*

Reports of infringements of the abovementioned provisions in court publications are usually investigated immediately and the appropriate remedial measures taken where necessary. Private individuals who make such prohibited publications are subject to the general rules of private law, which may under certain circumstances provide for the right to removal or withdrawal.

– *In the case of databases, is there a procedure for the automatic suppression of personal data?*

Court rulings intended for publication in the case-law database are rendered anonymous by means of appropriate markings using macros.

- *Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?*

Reports of infringements of the abovementioned provisions in court publications are usually investigated immediately and the appropriate remedial measures taken where necessary.

Penal Code

Breach of Official Secrecy

§ 310 (1) A civil servant or former civil servant who discloses or utilizes a secret with which he has been entrusted or to which he has gained access exclusively by virtue of his office and the disclosure or utilization of which might injure a public interest or a legitimate private interest shall be punished by imprisonment not exceeding three years where the offence is not liable to a more severe sentence under other provisions.

(2) Whosoever, as member of a committee pursuant to Article 53 of the Federal Constitution or of a standing sub-committee set up pursuant to Article 52a of the Federal Constitution, or as a person entitled to attend the deliberations of such committees, discloses or utilizes a secret to which he has gained access in a confidential meeting and the disclosure or utlization of which might injure a public interest or a legitimate private interest shall likewise be punished.

(2a) Whosoever – even after leaving office or employment – as an official or employee of the European Police Office (Europol), as a liaison officer or as a person under a particular obligation of discretion (Article 32(2) Europol Convention, Austrian Law Gazette (BGBl.) III, No 123/1998) discloses or utilizes a fact or opportunity to which he has gained access exclusively by virtue of his office or activity and the disclosure or utilization of which might injure a public interest or a legitimate private interest shall likewise be punished.

(3) Should the offender disclose an official secret relating to facts which represent a threat to the constitution (§ 252(3)), he shall only be punished if he acted with the intention of injuring private interests or harming the Republic of Austria. An erroneous assumption as to facts which represent a threat to the constitution shall not exempt the offender from punishment.

Offences taking advantage of office

§ 313 Should a civil servant, by taking advantage of an opportunity granted by virtue of his office, commit an offence which is otherwise also liable to punishment, the maximum possible prison sentence or fine may be increased by 50%. The term of imprisonment may nevertheless not exceed twenty years.

Federal Constitution

Article 20 (1) Temporarily elected officials or appointed professional officials shall be responsible for the administration under the direction of the highest authorities of the Federation and of the States in accordance with the law. Unless otherwise provided by the constitution, they shall be bound by the instructions of their superiors and shall be accountable to the latter for their official activity. A subordinate official may refuse to follow instructions if they were issued by an official acting outside his sphere of competence or if compliance with them would contravene provisions of criminal law.

(2) Where, for the purposes of a decision at the highest instance, a collegiate body has been set up by Federal or State law, the decisions of which, are by law not subject to repeal or amendment by administrative means and of which at least one member is a judge, the other members of that collegiate body shall likewise not be bound by any instructions in the execution of their duties.

(3) Unless otherwise provided by law, all officials entrusted with administrative duties relating to the Federation, the States or the districts and officials of other public-law bodies shall be under an obligation of discretion concerning all facts which come to their knowledge exclusively through their official activity and the confidentiality of which is necessary in the interests of maintaining public peace, order and security, of general national defence or of foreign relations or in the economic interest of a public-law body, or for the preparation of a ruling or in the overriding interest of the parties concerned (official secrecy). The official obligation of discretion shall not apply to officials appointed by a general representative body vis-à-vis that representative body where the latter expressly demands the information concerned.

(4) All officials entrusted with administrative duties relating to the Federation, the States or the districts and officials of other public-law bodies shall be bound to provide information concerning matters within their sphere of competence unless prevented from doing so by a legal obligation of discretion; professional representations shall be bound to provide information to their own members only and solely to the extent that this does not hamper the proper discharge of their legal duties. Legislation on and the execution of detailed rules concerning officials of the Federation and in the field of self-government as covered by Federal legislation shall be a matter for the Federation. Framework legislation on detailed rules concerning officials of the States and districts and in the field of self-government as covered by legislation of the States shall be a matter for the Federation, while the relevant implementing legislation and execution shall be a matter for the States.

Supreme Court Act

Entscheidungsdokumentation Justiz (case-law database)

§ 15 (1) The Federal Minister for Justice shall set up a generally accessible database (*Entscheidungsdokumentation Justiz* – case-law database) which shall contain the following:

1. rulings of the Supreme Court (full text) except for rejections of remedies without further grounds being given and
2. rulings prepared pursuant to § 14 (1) (Constitutional Court decisions on jurisdiction) and other texts.

In case of doubt, the decision shall lie with the president of the relevant chamber with regard to Constitutional Court decisions on jurisdiction, and otherwise with the head of the Office of the Supreme Court (*Evidenzbüro*).

(2) When making a ruling in cases in which the proceedings were conducted without a public hearing of all instances, the adjudicating chamber may order that the ruling (full text) shall not be published in the database if the anonymity of those concerned cannot otherwise be guaranteed.

(3) The Federal Minister for Justice may determine by order, according to the technical and human resources available and with due regard for simple and economic management and for protection against misuse, in particular,

1. what transmission agencies should be set up for queries, and
2. what conditions must be observed for secure operation of the case-law database.

(4) In the case-law database, names, addresses and, where necessary, place names which allow inferences to be drawn regarding the case concerned shall be rendered anonymous by the use of letters, numbers or abbreviations without impeding the intelligibility of the decision.

(5) Instructions pursuant to paragraph 4 shall be adopted by the adjudicating chamber when making rulings, and by the President of the Supreme Court in the case of rulings made before 1 January 1999.

(6) The Federation shall be liable for damage caused by the use of automatic data-processing due to errors in the management of the case-law database. There shall be no liability where the damage was caused by an unavoidable event due neither to an error in the design nor to a failure in the resources of the automatic data-processing system. Otherwise the law on official liability shall apply.

POLAND

The principle of openness – general remarks

Openness of judicial proceedings is one of the general principles common to states whose legal systems are founded on rule of law and respect for human rights and fundamental freedoms. This principle is expressly guaranteed by the European Convention of Human Rights, which provides in art. 6 that everyone is entitled to a fair and **public** hearing. Such a provision clearly results from the constitutional traditions of democratic states. The Republic of Poland demonstrated its respect for those values throughout its historical past, as well as in the period after 1989 when its attachment to the legal standards of democratic Europe has been firmly approved.

The principle of openness, as the emanation of the high quality of a legal system, is inscribed in The Polish Constitution of 1997 in article 45 thereof, which provides that everyone shall have the right to a fair and public hearing of his case, without undue delay, before a competent, impartial and independent court. The exceptions to this rule may be made for reasons of morality, state security, public order or protection of the private life of a party, or other important private interest. The public announcement of judgments is also constitutionally guaranteed.

The constitution guarantees of the principle of openness are balanced by the limitations thereof, whose objective is to reconcile the transparency of public life with the right to privacy. Consequently, according to article 51 of the Constitution:

1. No one may be obliged, except on the basis of statute, to disclose information concerning his person.
2. Public authorities shall not acquire, collect or make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute.

4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.
5. Principles and procedures for collection of and access to information shall be specified by statute.

The issue of personal data protection is regulated, among others, in the Code of civil procedure, Code of criminal procedure, Law on the Protection of Personal Data (below referred to as the PPD Law), Press Law, and Law on the Access to Public Information.

According to article 27.1 of PPD Law, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, judgments on penalty, fines and other decisions issued in court or administrative proceedings, is prohibited

Detailed solutions

The general contours of the principle of openness, as provided in international instruments and the Constitution, are further developed on the level of statutes and resolutions.

The legal doctrine defines two aspects of the principle of openness – internal and external one. The crucial feature of the internal openness is the authorization of the Parties as well as their defence counsels, attorneys, legal representatives and statutory agents to examine the files pertaining to the case and to copy them (art. 156 of the code of criminal procedure).

However, with a view to protecting legal data of defendants, these records may be made accessible to other persons only with the consent of the president of the court (external openness). This provision is of vital importance as regards the journalists' access to legal data. In this context it is necessary to balance the need of transparency of activities of state organs with the legitimate protection of personal data. Therefore the consent to examine the files is not equivalent to any authorization to publish information included in these files.

Consequently, it needs to be emphasized that, according to Press Law of 1984 personal data and image of parties persons participating in the proceedings in progress may not be published in press unless the consent of these persons is given. However, this prohibition may be lifted by a competent prosecutor or a competent court if "the vital social interest" so requires.

The interest of proceedings and the protection of data require that the limitations to the principle of openness should be stronger during the preparatory proceedings. For this reason, the access to data for participants, unless otherwise provided by law, requires permission by the person conducting the preparatory proceedings for the inspection of files of the preparatory proceedings in progress, making copies and photocopies of the same by parties, defence counsels, legal representatives and statutory agents, and for the issuance of certified copies. With the permission of the state prosecutor, access to files in the pending preparatory proceedings could be given to other persons.

The aforementioned frame of regulations pertaining to access to data seems to offer a balanced approach to the principle of openness where both the interest of the justice system and the protection of individuals are duly considered.

Moreover, the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation is reflected in provisions regulating the open character of a trial. The openness is again the general rule, to which the exception are permitted in specified circumstances, such as in case of a motion from the state prosecutor for discontinuance of the proceedings due to the non-accountability of the perpetrator and for applying a precautionary measure or in a case of defamation and calumny; on a motion from the injured, however, the hearing is held in open court. By the decision of the court, the public may be excluded from the trial in case of the possible disturbance of public order, offence of decency, disclosure of circumstances, which in consideration of significant state interests should remain secret, or infringement of important private interests. The court may also exclude the public from all or part of the hearing also when so required by a person which brought a motion to prosecute or when at least one of the accused is a minor.

To the end of the realisation of substance of the principle of openness, the judgement is announced in open court (if all or part of the trial has been held in closed session, the announcement of the statement of reason for the judgement may be also made in closed session).

The rules of the access to data in civil case do not introduce significant changes to aforementioned solutions. Nonetheless, it is worth mentioning that unlike the Code of criminal procedure, the Code of civil procedure does not describe these premises in detail, as basically they are included on the level of regulations.

In civil proceedings the hearing is, as a rule, public. However, the necessity to exclude the openness in certain situations has been respected by the legislator in such cases as: disturbance of public order or morality, the possible disclosure of circumstances covered by state or civil secret. The individual consideration of parties may also be the reason of the exclusion of a full public character of a trial, e.g. when: the trial touches upon the details of matrimonial or family life.

Publication of legal data

Solely the judgements of appellate courts and of the Supreme Court are published in the special journal. It is necessary to point out that in every case the data which might enable the data identification of parties is removed from these publications (solely the initials remain). The additional means of ensuring anonymity is the removal of the name of a town which is a site of a court which passed a judgement (solely a first letter remains).

The Law on the Protection of Personal Data of 1997 prohibits the transformation of personal data pertaining *inter alia* to court judgments (the law defines "the personal data" as any information regarding a person who is identified or possible to identify). The list of premises where this prohibition is lifted is of an exhaustive character, which contributes to the reconciliation of the transparency of public life with the legitimate protection of personal informations. Provisions of this law (whose infringement may be sanctioned by criminal sentence) seems to be a sufficient guarantee of a protection of data of subjects of court proceedings.

Detailed answers to selected questions, based on the PPD Law (and its amendments)

To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?

According to the appropriate provisions of rules of procedure only the parties of judicial proceedings receive judicial decisions. The decisions of the Supreme Court are published but personal data are suppressed (only first letter of a name is listed). The data that are published are outside the scope of definition of "personal data" as it has been put in the Directive 95/46/EC (art. 2 (a)).

The definition of personal data is stated in art. 6 of PPD Law of 29 August 29 1997
(consolidated text: Journal of Laws of 2002 No 101, item 926 with later amendments)

„art. 6 1. Personal data shall mean any information relating to an identified or identifiable natural person. 2. An identifiable person is the 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. 3. A piece of information shall not be regarded as identifiable where the identification requires an unreasonable amount of time, cost and manpower."

Are they eliminated in every case or only at the request of the person concerned?

Taking into account the above the question is not applicable.

(protection may result from art. 23 of the Civil Code (general provisions))

Is the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation accepted? To what extent?

The amendment to the PPD Law in art. 23. 1 (5) states that that the processing of data is permitted only if processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject." Art. 3a.2 provides that provisions on protection of personal data are applied if the processing of personal data carried out for journalistic purposes or the purpose of literary or artistic activity infringes the rights and freedoms of person concerned" (in line with art. 9 Directive).

It must be added that so far the Polish authority has not examined such cases.

Do different levels of protection exist for publication on the internet and in print?

There is a higher level of protection as regards computer systems. It is expressed on technical level where additional conditions are required in comparison with other manual systems. *Regulation of June 3, 1998 by the Minister of Internal Affairs and Administration as regards establishing basic, technical and organizational conditions which should be fulfilled by devices and information systems used for the personal data processing* (*Journal of Law of June 30, 1998, No. 80, item 521*) determines the fundamental technical and organizational requirements for the devices and systems of automatic processing of personal data.

§2

In order to have security of data appropriately managed within the computer system, the controller before starting to process personal data, is obliged to:

1) *define aims, the strategy and the policy of data security within computer systems in which personal data are processed,*
2) *identify and analyze any danger and risk to which personal data processing may be exposed,*
3) *define needs as regards security of personal data files and computer systems including the cryptographic protection of personal data, in particular during their delivery by means of devices used for data transmission,*
4) *define security measures appropriate to any danger and risk,*
5) *screen functioning of security measures to be implemented in order to protect and thereupon process personal data,*
6) *work out and implement a training program as regards the security of data within computer systems,*
7) *detect and react appropriately if any violation of security, either of personal data or of computer systems, has been revealed.*

§3

The controller appoints a person, hereinafter referred to as "an administrator of information security", who is responsible for personal data security within the computer system, in particular for counteracting against making the data processing systems be available for unauthorized persons and for taking appropriate actions where a breach of the security system has been revealed.

Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes.

It needs to be pointed out that pursuant to article 25.2.3 of the PPD Law, where the data have not been obtained from the subject, the controller is not obliged to fulfill the information obligation laid down in art. 25 .1 of PPD Law if the controlled data are necessary for scientific, didactic, historical, statistic or public opinion research, provided that the processing of such data does not violate the rights or freedoms of the data subject, and the fulfilment of the terms and conditions determined by paragraph 1 would involve disproportionate efforts or endanger the success of the research.

According to article 26.2 of PPD Law the processing of data, for the purpose other than intended at the time of data collection is allowed provided that it does not violate the rights and freedoms of the data subject and is done for the purposes of scientific, didactic, historical or statistical research.

Can the unauthorized or prohibited publication of identifiable references lead to criminal or civil liability?

As it comes to criminal liability it is stipulated accordingly in art. 49 and 51 of the PPD Law.

Article 49

1. *A person, who processes personal data from a data filing system where such processing is forbidden or where he is not authorized to carry out such processing, shall be liable to a fine, a partial restriction of freedom or a prison sentence of up to two years.*
2. *Where the offence mentioned at point 1 of this article relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, party or trade-union membership, health records, genetic code, addictions or sexual life, the person who processes the data shall be liable to a fine, a partial restriction of freedom or a prison sentence of up to three years.*

Article 51

1. *A person who, being the controller of a data filing system or being obliged to protect the personal data, discloses them or provides access to unauthorized persons, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to two years.*
2. *In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.*

For the time being the sanctions mentioned above have not been applied.
As regards the civil liability it is stipulated by art. 23 of the Civil Code.

In the case of databases, is there a procedure for the automatic suppression of personal data?

According to art. 26.1 (4) of the PPD Law the controller performing the processing of data should protect the interests of data subjects with due care, and in particular to ensure i.e. that the data are kept in a form which permits identification of the data subjects no longer than it is necessary for the purposes for which they are processed. It means that after the necessary period the data should be erased.

The Article 35 also should be mentioned in this regard as in case the data subject proves that the personal data relating to him/her are not complete, they are outdated, untrue or collected with the violation of the act, or in case they are no longer required for the purpose for which they have been collected, the controller shall be obliged, without undue delay, to amend, update, or correct the data, or to temporarily or permanently suspend the processing of the questioned data, or **to have them erased from the system**.

Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?

In this regard art. 18 of the PPD Law is appropriate as it gives power to the Inspector General *ex officio* or following a motion of the data subject in case the inspection reveals any breach of the provision on personal data protection to order the controller by means of an administrative decision, to restore the proper legal state, and in particular: to remedy the negligence, to complete, update, correct, disclose, or not to disclose personal data, to apply additional measures protecting the collected personal data, to suspend the cross-border flow of personal data, to safeguard the data or to transfer them to other parties, to erase the personal data.

It is also important to add that in case the Inspector General for Personal Data Protection has competence to examine other bodies (so far the activities of carried out by the Police and revenue offices has been examined). However, the Inspector General can not monitor the enforcement of substantive and procedural provisions. This has been confirmed by the Supreme Court in its judgement of 2 March 2001 (ref. II S.A. 401/00). The Supreme Administrative Court stated that the Inspector General is not the body entitled to monitor or supervise correctness of enforcement of substantive and procedural law in cases which are covered by the scope of terms of reference of other bodies, services or courts whose judgements shall be legally appraised in the course of instance or in other way which is defined by other appropriate procedures.

Irrespective of the above, it needs to be stressed that pursuant to art. 43.1.2 of the PPD Law, the obligation to register data filing systems shall not apply to the controllers of such data which is processed by relevant bodies for the purpose of the court proceedings. Moreover, pursuant to art. 43.2 of the PPD law as regards data filing systems containing data collected as a result of inquiry procedures held by officers of the bodies authorized to conduct such inquiries processed by Homeland Security Agency, Intelligence Agency or Military Information Services, the Inspector General is not entitled to carry out prior check to notification.

PORTUGAL

The Portuguese delegation would reply to the questions put by the Italian delegation in 14455/03 JURINFO 19 as follows:

- Use of new information technology applications is nowadays essential in seeking to modernise the justice system.

  Law No 67/98 of 26 October 1998 transposes into domestic law 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.

  That legislation requires processing of personal data to be carried out transparently and with strict respect for privacy and for civil rights, liberties and fundamental guarantees; in particular, it stipulates that personal data may be processed only "**with the data subject's clear consent**" and **prohibits** processing of "**sensitive data**", while setting out exceptions (Articles 6 and 7).

  Controllers of databases containing personal data are required to have their databases regulated by separate legislation, reflecting the provisions of personal data protection law, after consulting the National Data Protection Commission (CNPD).

Since the 1980s, the Ministry of Justice has been taking various steps to disseminate knowledge of the law, particularly legal literature and case law, among judicial practitioners, lawyers and others with an interest in access to such information.

For that purpose, legal databases were established, agreements reached with those interested in access to information and the necessary passwords supplied for consulting data.

In the late 1990s, with the spread of information and communications technology, the information in those databases was then made available on the Internet, without any of the previous access restrictions.

Such access for a much broader public was regarded as a legitimate, unimpugnable objective, with entitlement to obtain legal information being considered a basic civil right.

However, this gave rise to a variety of concerns relating specifically to the individual right to personal and family privacy.

The individual right to privacy could be encroached upon, as full-text judgments named individuals, showed their status in proceedings and might reveal criminal offences and many private personal and family details.

In order to get around that problem, the Ministry of Justice sought an opinion from the National Data Protection Commission concerning the procedures needed, in establishing and operating legal databases, so as to ensure strict, effective compliance with personal data legislation.

The Commission held that the texts of judgments should not include the identity of the individuals involved or any other data or information which might enable them to be identified without very laborious or time-consuming efforts; this could even apply to locations or dates of occurrences and addresses of individuals involved.

That finding has been heeded, with the adoption, in establishing and operating legal databases available via the Internet, of procedures for the removal of personal data from past judgments and for the omission of such data from future judgments.

- The procedures followed for the removal of individual identity details from judicial decisions do not curtail availability of information, as they do not impair readers' understanding of the text, and so the right to obtain legal information is upheld.

- The procedures for ensuring anonymity in legal databases are manual ones.

- The Ministry of Justice does have other programmes for processing of personal data held in databases. Those databases are regulated by specific legislation, after the National Data Protection Commission has given its opinion; for disclosure of data, it is specified that information may be supplied for statistical or scientific research purposes, with the database controller's express permission, provided the data subjects are not identifiable.

- As regards civil liability, under current legislation, anyone harmed by unlawful processing of data or by any other infringement of personal data protection law is entitled to claim damages from the party responsible.

- For the case-law databases kept by the Ministry of Justice, there is no provision for removal of information or correction of personal data at the data subject's request.

- The rules governing some Ministry of Justice databases in which personal data are processed do entitle data subjects, upon application to the database controller in writing, to have their details updated or corrected, if inaccurate, or deleted, if improperly recorded.

- It is for the National Data Protection Commission, with its powers as an independent administrative authority attached to parliament, to respond to requests from any parties for protection of their rights and freedoms and to consider individual complaints, appeals or petitions.

FINLAND

To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?

There is no direct reference to judicial decisions in the Personal Data Act (523/1999), but the general principles of the Act make it clear that the court judgments should protect anonymity.

Are they eliminated in every case or only at the request of the person concerned?
They are eliminated in every case.

For what purposes do the rules impose the removal of references that would make identification possible?
For the protection of the individual.

Is the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation accepted? To what extent?
According to the Personal Data Act, the citizen's right to information does not constitute any exceptions to the privacy of the individual.

Legal data is often published in periodicals intended for the general public or in publications for lawyers and other members of the legal profession. Is the anonymity criterion applied in such cases too?

Yes

Do different levels of protection exist for publication on the internet and in print?

No.

Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes. Are there rules governing such cases, which impose restrictions on their use or discretion on those who process the data or on researchers?

Yes, the rules are included in Section 14 of the Personal Data Act, (Section 14 — Research):
(1) Personal data may be processed for purposes of historical or scientific research also for a reason not referred to in section 8(1), if:

> *(1) the research cannot be carried out without data identifying the person and the consent of the data subjects cannot be obtained owing to the quantity of the data, their age or another comparable reason;*
>
> *(2) the use of the personal data file is based on an appropriate research plan and a person or a group of persons responsible for the research have been designated;*
>
> *(3) the personal data file is used and data are disclosed therefrom only for purposes of historical or scientific research and the procedure followed is also otherwise such that the data pertaining to a given individual are not disclosed to outsiders; and*
>
> *(4) after the personal data are no longer required for the research or for the verification of the results achieved, the personal data file is destroyed or transferred into an archive, or the data in it are altered so that the data subjects can no longer be identified.*

(2) The provision in paragraph (1)(3) does not apply if the procedure in that paragraph is manifestly unnecessary for the protection of the privacy of the data subjects owing to the age or quality of the data in the personal data file.

(3) The provisions in paragraph (1) apply in a supplementary manner where the processing of the personal data is based in section 8(1).

Can the unauthorised or prohibited publication of identifiable references lead to criminal or civil liability?

Yes, according to the Section 47 of the Personal Data Act, (Section 47 — Liability in damages):

(1) The controller is liable to compensate for the economic and other loss suffered by the data subject or another person because of processing of personal data in violation of the provisions of this Act.
(2) Otherwise the provisions in chapter 2, sections 2 and 3, chapter 3, sections 4 and 6 and chapters 4, 6 and 7 of the Damages Act (412/1974) apply to the liability in damages.

In addition, according to the Section 48 of the Personal Data Act, (Section 48 — Penal provisions):

(1) The penalty for a personal data offence is provided in chapter 38, section 9 of the Penal Code (39/1889) and for breaking into a personal data file in chapter 38, section 8 of the Penal Code. The penalty for a violation of the secrecy obligation referred to in section 33 is provided in chapter 38, section 1 or 2 of the Penal Code, unless the act is punishable under chapter 40, section 5 of the Penal Code or a more severe penalty is provided in another Act.

(2) A person who intentionally or grossly negligently and contrary to the provisions in this Act:

(1) fails to comply with the provisions on the definition of the purpose of the processing of the personal data, the drawing up of the description of the file, the information on data processing, the rectification of the file, the right of the data subject to prohibit the processing of data or the notification of the Data Protection Ombudsman;

(2) provides false or misleading data to a data protection authority in a matter concerning a personal data file;

(3) breaks the rules or regulations on the protection and destruction of personal data files; or

(4) breaks a final order issued by the Data Protection Board on the basis of section 43(3),

thus compromising the protection of the privacy of the data subject or his/her rights, shall be sentenced for a personal data violation to a fine, provided that a more severe penalty is not provided in another Act.

Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity be amended?

Yes

In the case of databases, is there a procedure for the automatic suppression of personal data?
Yes.

Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?

Yes.

DENMARK

Question 1+2)

- There exists no general obligation to anonymity in the Danish law. In general judicial decisions can be published. Publication is not allowed if it violates the integrity of privacy as protected by as well the criminal code (section 264 d), the European Convention on Human Rights (article 8) and The Act on Processing of Personal Data (based on directive 95/46 EF which limits private electronic publication, for instance on the internet).

The Act on Processing of Personal Data provides in section 6 that a private person are not allowed to publish judicial decisions unless the data subject has given his explicit consent or processing is necessary for the performance of a task carried out in the public interest. Sensitive data[1] must not be published unless the data subject has given his explicit consent or the processing relates to data which have been made public by the data subject.

The provisions in the Act on Processing of Personal Data lead to a principal rule: a right to anonymity.

Although a series of exceptions do exist which apply to the following situations or individuals:

1) **Legal information systems:** The Act on Processing of Personal Data provide in section 9 that data may be processed where the processing is carried out for the sole purpose of operating legal information systems of significant social importance and the processing is necessary for operating such systems. The authorisation of the Data Protection Agency shall be obtained (cf. section 50) and the supervisory authority may lay down more detailed conditions concerning the processing operations. In practice the supervisory authority has decided that anonymity in the publication of judicial decisions is required in a number of situations for example in criminal cases, matrimonial cases, tax cases and actions for damages.

[1] personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life cf. section 7, and data about criminal records, serious social problems and other purely private data cf. section 8

2) **The information databases of the mass media:** The information databases of the mass media are not regulated by The Act on Processing of Personal Data, but by the Act on information databases of the mass media. If an information database is accessible to the public it must be reported to the Press Council and the Data Protection Agency. Private data regarding individuals, may not be stored longer than a 3 year period, after the event that caused the filing of the information. The 3 year limit for storing sensitive data does not apply, if it is found that the public interest in access to data is of such high interest that the individuals right to anonymity should give way for the freedom of information. The mass media hereby has the possibility to publish judicial decisions, regardless of the possible identification of the individual, as long as the publication is in compliance with the law of media liability.

3) Civil cases: In matrimonial cases, cases concerning custody, paternity and adoption without consent, the identity of the individual(s) involved in the judicial decision must not be published along with the publication of the judgement cf. The Administration of Justice Act (sections 453, 456 m and 475 g). The penalty for such violation is punished with fine and in cases concerning matrimony, custody and paternity even imprisonment in severe violations in up till 6 months cf. The Administration of Justice Act (sections 453, 456 m and 475 g).

4) Criminal cases: In cases concerning sexual crimes the identity of the injured party must not be published cf. the Administration of Justice Act (section 1017 b, 1). Again violations are fined. The police is entitled to publish the identity of the injured party, when the publication is necessary for the detection of the crime or when it is necessary for protection of the public interest.

Based on the report by The Administration of Justice Council (No. 1427/2003), The Ministry of Justice has produced a bill (No. 23/2003 on October the 8. 2003), which was enacted by the Danish Parliament, on the 16. of March 2004, concerning publicity in the administration of justice. The law comes into force on the 1. of July 2004 and stipulates a general obligation to anonymity of the individuals and legal persons involved in any criminal cases.

Judicial decisions may only be published, if identity and identifiable references regarding the suspects, the defendants, the injured parties or witnesses, do not appear in the publication cf. The Administration of Justice Act (section 1017 d, 1). Violations of the anonymity results in criminal liability according to the criminal code (cf. provision 23). To the mass media it applies a special liability confirmed by the code of mass media. Legal information systems under The Act on Processing of Personal Data section 9 are excepted from the law cf. The Administration of Justice Act (sections 1017 d, 2).

Question 3)

The purposes of the obligation to anonymity in the publication of judicial decisions are to respect the privacy, integrity and dignity of the individual as protected by the criminal code (section 264 d), The European Convention on Human Rights (article 8) and The Act on Processing of Personal Data according to which a private person is not allowed to publish judicial decisions unless the data subject has given his explicit consent.

Question 4)

The Danish legal system respects and protects the citizens right to privacy, integrity and dignity[1]. The right is not absolute. The Act on Processing of Personal Data states in section 2 that the Act does not apply where this will be in violation of the freedom of information and expression, cf. Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The citizen`s right to information may therefore take priority to the individuals right to privacy.

Question 5)

Legal data published in periodicals intended for the general public and in publications for lawyers and other members of the legal profession: If journals and publications are included by the Act on Processing of Personal Data the individual preserve its right to anonymity.

[1] as stipulated in the criminal code (section 264 d), The European Convention on Human Rights (article 8) and the requirements of The Act on Processing of Personal Data.

Question 6)

If the publication is in accordance with the requirements of the Act on Processing of Personal Data, the individual enjoys the same protection regardless if the publication is printed or electronic on the internet.

Question 7)

It is allowed to process personal data used for statistical or scientific research purposes. The Act on Processing of Personal Data requires that the processing is necessary (cf. section 10). The data may not subsequently be processed for other than statistical or scientific purposes. The data may only be disclosed to a third party with prior authorisation from the supervisory authority and the supervisory authority may lay down more detailed conditions concerning the disclosure. Failure to comply is subject to criminal liability.

Question 8)

The unauthorized or prohibited publication of identifiable references which violates The Act on Processing of Personal Data can lead to civil liability as well as criminal liability (cf. section 69 + 70).

Question 9)

If a publication violates The Act on Processing of Personal Data the individual always has the right to demand correction of the data. Section 37 states that the controller at the request of the data subject shall rectify, erase or block data which turn out to be inaccurate or misleading or in any other way processed in violation of law or regulations. The controller has, at the request of the data subject, an obligation to notify the third party to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with subsection. However, this shall not apply if such notification proves impossible or involves a disproportionate effort. The controller is also subject to civil/criminal liability.

The individual can file a complaint to the Data Protection Agency, which in accordance with section 59 may order a private data controller to discontinue a processing operation which may not take place under this Act and to rectify, erase or block specific data undergoing such processing. Failure to comply this will result in civil/criminal liability.

Question 10)

There is no procedure for the automatic suppression of personal data. The suppression of personal data is individual and depends on the specific situation of processing of personal data. Section 5 states that the data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed.

The Data Protection Agency exercises the supervision and control with any processing of personal data regarding the The Act on Processing of Personal Data. The controller shall therefore prior to the commencement of any processing of data notify the Danish Data Protection Agency (cf. section 48) and the authorisation of the Data Protection Agency shall be obtained (cf. section 49).

The Data Protection Agency is supervising ex officio or on basis of a complaint from a citizen that the processing of the information is done in accordance with the law (cf. section 58).

ESTONIA

To what extent does the law protect anonymity by eliminating names or identifiable references from judicial decisions that are published?

According to Estonian law judicial decisions are public information, therefore all the names are public. Estonian Data Protection Inspectorate made a proposal to publish on the website initials instead of names, but so far there are no amendments made.

- Court hearing of matter is public;

- Composition of the panel of court which hears a matter shall be made public;

- A court may declare that a session or a part of it will be held *in camera*:

  - to maintain a state or business secret;
  - to protect moral or the privacy or family life of a person;
  - to maintain the confidentiality of messages sent or received by a participant in the proceeding by post, telegraph, telephone or other commonly used means;
  - to maintain the confidentiality of adoption;
  - in the interests of minor;
  - in the interests of the administration of justice;
  - to hear a person who is up to 15 years of age or who has a mental disorder or mental disability.

- At a court session held *in camera* the participants in the proceeding and, if necessary, also the witnesses, experts, interpreters and translators shall be present at the hearing of the matter. Court officials, trainees, and persons with a particular reason therefore may also be present at a court session held *in camera* with the permission of the presiding judge.

- A person of up to 15 years of age who is neither a participant in the proceeding nor a witness may be present at a court session with the permission of the court.

- The provisions of courts procedure shall be observed in court sessions held *in camera*. Judgments in court sessions held *in camera* shall be made public unless the interests of a minor or a spouse require otherwise.

- A court shall not disclose a state secret which has become known to the court in the course of a court proceeding.

- A person with a legitimate interest has the right to examine the court records concerning a court matter which has been adjudicated by a court if the court's decision has entered into force. The court records shall not be examined if the matter was heard in a session held *in camera* or if a basis specified in afore for declaring that a session be held *in camera* existed. A judge shall verify the existence of such basis for declaration that a session be held *in camera* before giving permission to examine a file.

- Are they eliminated in every case or only at the request of the person concerned?

See the answer afore.

- For what purposes do the rules impose the removal of references that would make identification possible?

Judgments in court sessions held *in camera* shall be made public unless the interests of a minor or a spouse require otherwise.

- Is the principle of a fair balance between the citizen's right to information and the right of the person named to defend their reputation accepted? To what extent?

See the answer afore

- Legal data is often published in periodicals intended for the general public or in publications for lawyers and other members of the legal profession. Is the anonymity criterion applied in such cases too?

Yes

- Do different levels of protection exist for publication on the internet and in print?

No

- Personal data allowing a person to be identified are sometimes used for statistical or scientific research purposes. Are there rules governing such cases, which impose restrictions on their use or discretion on those who process the data or on researchers?

In such cases the data controller must register (notify) sensitive data processing (according to the Personal Data Protection Act) in the Estonian Data Protection Inspectorate.

- Can the unauthorised or prohibited publication of identifiable references lead to criminal or civil liability?

Yes

- Does the person whose identifiable data are included in a judgment have the right to request their removal, that they be updated or that the name or any other reference which has in some way infringed the rules on anonymity be amended?

Yes

- In the case of databases, is there a procedure for the automatic suppression of personal data?

No

- Can the authorities be asked to intervene to amend or complete information containing identifiable references published in violation of laws on the protection of personal data or on respect for anonymity?"

Yes they can ask, but final decision making is up to the Government and Parliament

SWEDEN

Public access to courts is a cornerstone of the Swedish judicial system. With certain exceptions, court proceedings are open to the general public, and documents which are submitted to courts are also generally accessible. The principle is therefore that the public have access to both information on persons who are parties to or otherwise involved in proceedings (e.g. as witnesses) and the judgment or decision itself. However, there are a number of provisions concerning secrecy which apply to court-related information. The secrecy provisions applicable to various types of cases can vary depending on the interest which such secrecy is intended to protect. Some secrecy provisions stipulate absolute secrecy, while others are based on the principle that information should be publicly accessible.

In many cases, courts are obliged to comply with a secrecy requirement in cases where a piece of information comes from another court or authority which has classified the information in question as secret. At various occasions during proceedings, the court must examine whether or not secrecy should apply, e.g. during a hearing, or when a case is being decided. Information ceases to be secret if, for example, the information is published in a judgment or decision, unless the court has ordered in the judgment or decision that secrecy should apply. Such an order for secrecy does not normally apply to the operative provisions of the judgment or to the corresponding part of the decision. Unless the court has ordered secrecy, its decision is entirely public.

A person can ask a court not to disclose his personal data, but it is for the court to decide whether there are grounds for prescribing secrecy. It is very unusual for data concerning a person's identity to be subject to secrecy in judgments or decisions.

Directive 95/46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data has been implemented in Sweden by the Personal Data Act (PDA). The Act applies to all forms of processing of data which can be linked to living natural persons and which are wholly or partly automated. The Act also covers the manual processing of personal data in cases where such data are included in or are intended to be included in a register. National courts may process personal data where that is necessary in order to fulfil a legal obligation, for example, or in order to be able to perform tasks in connection with the exercise of public authority. In addition, "sensitive" personal data may be processed if such processing is necessary in order to establish legal claims. Judgments handed down by Swedish courts almost always contain personal data.

Where Swedish judgments are published on the Internet and such treatment cannot be regarded as being covered by the aforementioned court activities, a decision as to whether such treatment is permissible is based on an assessment of the importance of satisfying a justified interest as against the individual's interest in protection against violation of his personal integrity. On some occasions it may also be necessary to disseminate information in order to be able to perform a task of general interest.

Data processing of a type which is protected by the provisions of the Swedish constitution concerning the freedom of the press and the freedom of speech is excluded from the scope of the PDA. Nor does the PDA apply to the processing of data solely for journalistic purposes or for artistic or literary creations. To the extent that the handling of cases before the Swedish courts is covered by those exceptions, the processing of personal data (including "sensitive" data) is therefore permitted regardless of whether it is processed in writing or via the Internet. In the case of data processing for journalistic purposes or for artistic or literary creations, it is the aim rather than the form of such publication which determines the level of protection. It is not possible to remove personal data which have been published legally in writing or via the Internet. On the other hand, in cases where personal data have been published in violation of the PDA, it is possible to demand redress from the person responsible for processing the personal data in question.

The latter then himself decides whether the data should be corrected, blocked in such a way as to indicate that they are withheld and will not be issued to third parties, or deleted so that they cannot be reproduced. Any person responsible for processing personal data in violation of certain provisions of the PDA may be fined or imprisoned, but will not be held liable in minor cases. He will also be obliged to compensate the injured party for the damage to and violation of his personal integrity caused as a result of his personal data being processed in contravention of the PDA. Moreover, the Swedish authority responsible for monitoring compliance with the PDA, the Data Inspection Board, can order any person responsible for the unlawful processing of personal data to cease such activities under penalty of a fine, and may institute court proceedings if such processing continues.

With regard to case law, the Swedish Government's legal information system, www.lagrummet.se, currently publishes only brief references to interpreting judgments. Such references do not contain personal data or any other information which could identify persons involved in proceedings.

However, work is under way in Sweden to publish interpreting judgments in their entirety in the legal information system. Publication is expected to commence at the beginning of next year. In order to make this possible, legislation has recently been adopted which will enter into force on 1 December this year. The new provisions state that the legal information system must not contain any data which could be directly related to a living natural person. However, exceptions have been made for judges who have ruled in a case and for experts who have provided information in a case. Furthermore, names may be indicated if the court refers in a judgment to literature or foreign decisions. The new provisions also state that sensitive personal data may be included in the system. However, this applies only if such data are necessary in order to understand the decision. Sensitive personal data may sometimes be included if the decision in question relates precisely to such data. This may be the case, for example, if the dispute concerns the issue of membership of a trade union or persecution of an ethnic group. Sensitive personal data must be included if a case is to have any meaning in the types of examples in question.

In Sweden, every citizen has a personal number for the purposes of identification in various situations. Such personal numbers cannot appear in the legal information system.

Only a small number of courts publish decisions on the Internet on their own initiative. Where this does happen, in principle only the court's members and rapporteurs are named, together with any experts or authors.

The various private legal databases which exist in Sweden are not covered by the aforementioned provisions. Such databases are not subject to any specific rules concerning the protection of personal integrity, for example. Rather, they are covered by the general rules laid down in the Personal Data Act. However, a number of private undertakings do not apply the provisions of the Personal Data Act, instead invoking the Swedish Fundamental Law on Freedom of Expression in order to protect themselves when publishing legal cases in the databases. This can happen not only if the party responsible for the database has an editorial office for a periodical or is a news agency, but also in cases where the private undertaking has requested and obtained voluntary constitutional protection for its legal databases in the form of an "authorisation to publish". Publication is then governed by the provisions of the Fundamental Law on Freedom of Expression concerning radio programmes. This means *inter alia* that no advance monitoring may take place. However, the person responsible for publishing the database may be prosecuted for offences relating to freedom of expression in respect of a number of different types of activity. For example, persecution of an ethnic group, slander and insult may constitute offences relating to freedom of expression. There is no general definition of activities which are not permitted and constitute offences. This is determined by the courts on an individual basis.

UNITED KINGDOM

General

1. It is noted that the Italian delegation, in the light of recent legislative developments in Italy, wishes to compare the ways in which the principle of the right to privacy is applied in the sphere of legal data processing in the various member states. In particular, the Italian delegation is interested in learning how and to what extent anonymity is afforded to individuals in reports of judicial proceedings and in the electronic dissemination of such reports.

2. As noted in the Italian paper, the relevant EU legislation is Directive 95/46/EC of 24 October 1995. This Directive has been implemented in the UK by the Data Protection Act 1998 (c. 29) and subordinate legislation made under powers contained in that Act.

3. The implementation of the Directive has recently been reviewed by the Commission (in May 2003) and the report recommended no modifications to the Directive at this time. The operation of the Directive is kept under review by the working party established under Article 29 and it is suggested that this would be the appropriate body for discussion should any modifications to the Directive be proposed or any questions raised concerning its implementation.

Reporting of Legal Proceedings in the UK

4. It is a feature of open justice in the UK that, where judgments in legal proceedings are published, they are published openly to all. In particular, in precedent-based common law systems of justice, such as that of England and Wales, much greater weight is attached to court judgments than in civil law jurisdictions. Consistently throughout the UK the names of the parties or others involved in legal proceedings are not restricted unless there are good grounds for doing so (children, national security etc).

5. An exemption from the non-disclosure principles in relation to legal proceedings is specifically provided for in the Data Protection Act (section 35) and this is in accordance with the provisions of the Directive. The Act also contains special rules for the processing of personal data for the purposes of journalism, among other things. The UK would not wish to see any change to the present position without full discussion at the appropriate levels, domestic and EU, including the senior judiciary in the UK.

THE SPECIFIC QUESTIONS

6. The first five questions are answered in general terms by paragraphs 4 and 5 above. As has been noted, there are circumstances in which restrictions on identification may be imposed by rules of court or by judicial decision. There are also restrictions on public access to court documents. However, these are not to be seen as particular expressions of a general 'principle of privacy'. There is no special provision in relation to publication on the internet as opposed to print media (question 6). Subject to the foregoing, the answers to the remaining questions are as follows:

7. The seventh question concerns the use of personal data for statistical or scientific research purposes. Section 33 of the Data Protection Act provides for an exemption from the non-disclosure principles for these purposes, but subject to certain restrictions. For example, results of research or statistics may not be made available in a form which identifies the individual who is the subject of the data and data may not be processed in such a way as to cause substantial damage or distress to the subject.

8. The eighth question asks about liability. The general position is that breaches of the Act incur civil liability. However, the Act also provides for criminal penalties for the unauthorised obtaining or disclosure of information in certain circumstances.

9. Remedies are available under the Act if personal data is obtained, disclosed or otherwise processed in breach of its provisions. These include the issue of an enforcement notice by the Information Commissioner (who is the data protection supervisory authority) specifying the remedial steps to be taken or an order of the court requiring the rectification, blocking or destruction of inaccurate data. In limited circumstances, an individual has the right to seek to prevent the processing of personal data, even if the processing is perfectly lawful, where it would be likely to cause unwarranted substantial damage or unwarranted substantial distress to him or another person.

10. There is no provision for the automatic suppression of personal data in the case of databases.

11. See paragraph 9 above.