COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 October 2001

T-PD / CJ-PD (2001) 01
Bilingual/bilingue

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD) /
COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL (T-PD)

PROJECT GROUP ON DATA PROTECTION (CJ-PD) /
GROUPE DE PROJET SUR LA PROTECTION DES DONNÉES (CJ-PD)

17th meeting of the T-PD (8-10 October 2001)/
17e réunion du T-PD (8-10 octobre 2001)

39th meeting of the CJ-PD (10-12 October 2001)/
39e réunion du CJ-PD (10-12 octobre 2001)

CONTRIBUTIONS ON RECENT NATIONAL DEVELOPMENTS IN THE FIELD OF DATA PROTECTION / COMMUNICATIONS SUR LES DÉVELOPPEMENTS RÉCENTS INTERVENUS DANS LE DOMAINE DE LA PROTECTION DES DONNÉES AU NIVEAU NATIONAL

Secretariat Memorandum
prepared by the
Directorate General of Legal Affairs

Albanie

Une loi sur la protection des données à caractère personnel a été adopté. Pour plus de détails le site Internet www.instat.gov.al peut être consulté.

Austria

Social Security Card

A project has been started to equip all insured persons with chipcards to administer social security functions. The card will not carry medical data, only information to administer visits to doctors and hospitals as well as data concerning the status of insurance. The first cards will be issued in summer 2002.

At the end of November 2000, a decision was taken by the government that it should be possible to use the chipcard also as a "citizen card", especially as chipcards are capable of carrying a secure digital signature. The card could be used, for example, at any contact with the public authorities. Furthermore there is discussion on if and to what extent personal data could be stored on a voluntary basis.

A debate about the functionality of the card, the safety features and privacy implications is under way.

E-Commerce Legislation

The Ministry of Justice sent out the draft of a new E-Commerce law in July. At present the responses are being evaluated. The new law will implement Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

New Website

The Austrian Data Protection authorities have a new website: http://www.bka.gv.at/datenschutz/ .

Belgique

1. Législation générale sur la protection des données:

Depuis le 1er septembre 2001, et suite à la parution de son arrêté royal d'exécution, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel – dans sa version transposant la directive 95/46/CE – est entrée en vigueur dans toutes ses dispositions.

Nous noterons particulièrement que l'arrêté royal d'exécution précité, du 13 février 2001, s'est à plusieurs reprises, fortement appuyé sur la recommandation N° R (97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins statistiques du 30 septembre 1997.

2. Loi du 28 novembre 2000 relative à la criminalité informatique :

La Belgique s'est dotée d'une loi visant, d'une part, à réprimer différentes sanctions en matière informatique et fixant, d'autre part, différentes règles de procédure pénale spécifiques en la matière.

Parmi ces procédures, il y a également une disposition concernant la conservation, par les opérateurs de télécommunications, des données de trafic pendant une période d'une année minimum, en vue d'être mises ponctuellement à la disposition des autorités judiciaires dans le cadre de la poursuite des

infractions. Cette disposition a naturellement fait l'objet d'une controverse majeure parmi les experts en protection des données.

3. Réforme de la gestion de l'information dans le cadre de la réforme des services de police :

Dans le cadre de la réforme globale des services de police, la Belgique s'est également attelée à la réforme de la gestion de l'information de ces services.

Le défi est de taille puisqu'il consiste, pour l'essentiel, à intégrer l'information conservée – quelle que soit sa qualité – dans plusieurs milliers de fichiers et registres délocalisés en une seule banque de données nationale générale. Celle-ci devra servir aussi bien en matière de missions de police judiciaire que pour les missions de police préventive, elle devra servir aussi bien les services de police locale que les services de police fédérale.

Un groupe de travail composé de magistrats, de policiers, de gestionnaires fonctionnels d'informations, d'informaticiens et d'experts en protection des données s'est réuni intensivement pour construire le nouveau concept. Ce dernier a choisi, comme fondation, les principes de base consignés à l'article 5 de la Convention N° 108.

Par ailleurs, faisant suite un vœu formulé, en son temps, par la Commission de la protection de la vie privée, un organe de contrôle de la gestion de l'information au sein des services de police – faisant office de préposé à la protection des données – a également été crée.

Croatia

A Council of Europe seminar was held in Croatia in December 2000 in order to discuss the draft law on data protection. A new draft was sent to the Council of Europe's experts and it is almost ready to go before Parliament.

There is a draft law on electronic signature.

Czech Republic

Since October 2000, the Office for Personal Data Protection of the Czech Republic has started its regular work. At present the Office has 65 members of staff.

In February 2001 a nationwide census was started under the direction of the Czech Statistical Office. The Office for Personal Data Protection repeatedly criticized the methods and data structure of this census. The OPDP decided to delete two items of personal data collected in the census. The CSO took court action against the OPDP ruling.

On 9 July, the Czech Republic ratified Convention 108.

On 10 October, the Cabinet debated the signature and ratification of the Additional Protocol to Convention 108. The Czech Republic will (probably) sign it in November on the occasion of the Ministerial Session.

Further information is available on the Office's website: www.uoou.cz

Denmark

On 1 July 2000 the Act on Processing of Personal Data came into force in Denmark. An essential purpose of the Act was to implement Directive 95/46/EC on the protection of individals with regard to the processing of personal data and the free movement of such data. The meeting report from the 38th meeting in CJ-PD, (2000) 27 contains a short description of the main elements of the Act - one of which is ensuring a high level of data protection in relation to the individual. A translation of the Act can be found at www.datatilsynet.dk.

The new data protection legislation in Denmark has not influenced greatly in the way the Data Protection Agency (DPA) acts. The DPA will in other words continue to act upon a complaint or ex officio and is still empowered to demand disclosure of all information relevant to its duties which are to ensure compliance with the law. With proper identification the staff of the DPA is also admitted to any and all premises from which a file is operated without a court order.

Implementation of the Act in practice has caused a greatly increased workload for the DPA. In the period from the Act came into force until the end of August 2001 the DPA has received 9 034 new cases. A considerable number of these cases (approximately 6.970) are notifications from public authorities and private persons or bodies. An increase in the number of employees has been necessary, especially employees with a legal education as well as employees with technical knowledge. At the end of August 2001 the DPA counted 33 employees (contrary to 24 employees at the end of 1999). The DPA moved to Borgergade 28, 1300 København K on 1 November 2001.

The organization of the DPA has not been changed. The DPA still consists of a Council - Datarådet (the Data Council) and a Secretariat. The Council has laid down its own rules of procedure in statutory order of 15 December 2000 according to the Act on Processing of Personal Data.

The decisions made by the DPA are final and may not be brought before any other administrative authority. The decisions can, on the other hand, be brought before the courts, and complaints concerning the administration of the Agency can be addressed to the Parliamentary Ombudsman.

Along with the ordinary supervision of processing operations covered by the Act, the DPA now has several new tasks. The Danish government has initiated the process of promoting electronic civic service in the administration, and the DPA has undertaken the task of central validation body. Amongst other things the DPA gives advice in security matters as regards the protection of personal data, for example when the authorities establish self-service on the Internet.

The new Act requires the opinion of the DPA to be given prior to legislation and drawing up of new laws, orders and circulars containing regulations of importance for the protection of privacy.

Pursuant to the Act on Processing of Personal Data, the Ministry of Justice has issued 10 statutory orders. One of the orders concerns security of processing of personal data carried out for the public administration; another concerns the processing of personal data in the Central Criminal Register.

Since the new Act came into force the DPA has issued 4 public guidances. Most important is a guidance on the rights of the data subject, namely dealing with frequently asked questions concerning information to be provided to the data subject - a new right for the data subject in the Act on Processing of Personal Data. The remaining 3 public guidances concern notification of processing carried out for the public administration, disclosure to credit information agencies of data on debts to public authorities and the required security of processing of data in public authorities.

Neither the statutory orders nor the public guidances have been translated into English.

Finland

1. Data Protection Legislation

The amendment to the Personal Data Act taking account of the decision-making of the Commission of the European Communities in the field of transfer of personal data to third countries was accepted by Parliament in November 2000. The changes to the Personal Data Act (986/2000) entered into force on 1 December 2000.

The Law Protecting Privacy in Working Life (477/2001) was accepted by Parliament in June 2001 and entered into force on 1 October 2001.

2. The action of the Data Protection Ombudsman

The number of new cases recorded by the Office of the Data Protection Ombudsman in 2000 increased by nearly one third from the previous year.

This is explained *first of all* by the Office switching from telephone service to electronic customer service. Although the Office did not use electronic signatures, it also recorded cases brough before it by e-mail in accordance with the Act on the Openness of Government Activities (Openness Act).

Secondly, the contents of the cases show that controllers of registers are working actively to adapt their practices to the Personal Data Act. During the year under review, the principle of self-regulation, included in the Act, also manifested itself in drawing up codes of conduct. The number of resolved cases increased significantly in 2000: the number of decisions issued by the Data Protection Ombudsman increased by 33 per cent.

The level of data protection in Finland was assessed in several studies. In the spring, Statistics Finland published a report, which revealed that citizens have confidence in new technologies and do not show much concern for the level of their data protection. On the other hand, they want to know who collects and processes data concerning them and what the data are used for. Similarly citizens want to participate in decision-making concerning themselves. In connection with the implementation of the Schengen Treaty, an evaluation and inspection group consisting of representatives of the treaty nations visited Finland. Based on the group's report, the Schengen Joint Supervisory Body stated that Finalnd fulfils the requirements set for the level of data protection.

In their mutual contacts, businesses are increasingly switching over to the e-world, that is, electronic data transfer and commerce. Consumers, on the other hand, have been quite reserved in this respect. According to various studies, one of the most important reasons for this is that consumers are concerned about their data protection, often with just cause. The network world is a global world and the problems are global.

During 2000, the Data Protection Ombudsman issued opinions on 20 cases to prosecutors and courts of law on violation of data protection and data security.

France

Il y a deux projets de loi qui sont en train d'être examinés: un projet concerne la transposition de la Directive 95/46/CE en France et l'autre projet de loi concerne la société d'information.

Hungary

Revision of the Hungarian Data Protection Act has started. There is a new law on electronic signatures and transfer of official documents by electronic means. The new data protection commissioner has not yet been appointed.

Iceland

The new Data Protection Law was adopted on 23 May 2000. This new law substituted the former data protection law of 1995. A new bill on electronic signatures is being drafted.

On 1 January 2001, the Act on Privacy and Processing of Personal Data came into force in Iceland. The main purpose of the Act was to implement Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data.

A new institution was established (Data Protection Authority/"Personvernd"). The former institution (Data Protection Commission/"Tölvunefnd") worked until 31 December 2000.

The Data Protection Authority (DPA) has a homepage www.personuvernd.is. There an English translation of the Act can be found. The main element of the Act is to ensure a higher level of privacy as regards the processing of personal data.

The DPA consists of a Council and a Secretariat. The decisions made by the DPA are legally binding. They are final and cannot be brought before any other administrative authority. The decisions can on the other hand be brought before the courts, as well as complaints concerning the administration of the DPA can be addressed to the Parliamentary Ombudsman.

Ireland

Transposition of Directive 95/46/EC

Drafting of the Data Protection (Amendment) Bill is at a very advanced stage and it is expected that the Bill will be published in the near future.

As passage of the Bill through the Houses of Parliament may take some time following publication, it has been decided to expedite transposal of some of the provisions of the Directive, namely Article.4 (Scope) and Articles 25 and 26 (Transfers of Personal Data to Third Countries) by way of Regulations made under the European Communities Act, 1972. It is expected that these Regulations will come into force before the end of the year.

Reasons for Delay in Transposition of Directive 95/46/EC

The heavy legislation programme in the Department of Justice, an extensive consultation process in relation to the Bill (including a consultation paper issued by the Department) and the complexity of the legislation has delayed progress on drafting of the Bill.

Italy

1. Foreword

No significant legislative amendments were made in the period considered as regards Act N° 675/1996, on the processing of personal data. However, the activities aimed at supplementing and updating the relevant legislation continued and "horizontal" provisions were made that produced effects in terms of personal data protection. Further information can be found on the Garante's web site (www.garanteprivacy.it).

2. Main Regulatory Developments

a) Special importance should be attached to Act N° 127 of 24.03.2001 – *Postponing the Deadline Enabling Government to Pass Legislation in pursuance of Act N° 676/1996, on the Processing of Personal Data*[1] - which postponed the deadline for the Government to pass legislation on privacy as mentioned in Acts n° 676/1996 and 348/1998. Under this Act, the framework legislation applying to data processing can be supplemented until 31 December 2001, as regards those sectors where the general principles laid down in the 1996 DPA have to be specified or completed and this has not yet been done by Government, in whole or in part. The Act also provided for issuance, by 31 December 2002, of a consolidated text of the provisions concerning the protection of individuals and other entities with regard to the processing of personal data – including all the measures in force as well as such amendments and additions as will be deemed necessary to enhance coordination or else facilitate enforcement.

b) Act n° 325 of 03.11.2000 – *Provisions Concerning the Adoption of the Minimum Security Measures for the Processing of Personal Data Referred to in Article 15 of Act n° 675 of 31.12.1996*[2]- granted additional time, until 31 December 2000, to the entities that had not managed to adopt the so-called minimum security measures by 29 March 2000, on condition that they drafted a document bearing a certified date to describe (a) the specific technical and organisational requirements that had made it necessary to take advantage of the postponed deadline, (b) the arrangements that had been or were to be adopted and the main features of the adjustments on schedule, (c) the guidelines developed in order to fully implement security measures.

c) The adoption of the Code of conduct and professional practice applying to the processing of personal data for historical purposes[3] should be also highlighted; this was provided for in a legislative decree of 1999 (n° 281 of 30 July). The Code was aimed at ensuring that personal data acquired in connection with historical research, exercise of the right to study and information as well as the activity of archives would be used in compliance with data subjects' rights, fundamental freedoms and dignity – with particular regard to the right to privacy and personal identity.

3. Other Regulatory Developments

A few regulatory instruments were passed in the period considered that also produced significant effects on the processing of personal data. The most important among them are briefly described below:

[1] Official Journal n° 91, 19.04.2001
[2] Official Journal n° 262, 09.11.2000
[3] See the Provision by the Garante, n° 8/P/2001, as published on the Official Journal n° 80, 05.02.2001

a) Act n° 340 of 24.11.2000, including provisions on de-regulation and simplification of administrative proceedings. Under Article 3 thereof, an important instance of the public interest – as based on the definition laid down in legislative decree n° 135 of 11.05.1999, on the processing of special categories of data by public bodies – consists in direct consultation by either a public administrative agency or the manager of a public utility of the files held by the administrative body that is competent for issuing a given certificate in order to establish, ex officio, specific circumstances or qualifications or events or else verify the statements made by citizens in this regard.

b) Prime Minister's decree of 6 December 2001, concerning the 2001-2003 National Statistics Programme. The processing of personal data is referred to specifically in paragraph 1.3 of the Preamble, where the regulatory provisions are mentioned that underlie he purposes for which data may be collected as well as the safeguards for fundamental rights. In particular, reference is made to the information to be provided to data subjects, their right of access to personal data and the main precautions to be taken in processing sensitive data.

c) Act n° 397 of 07.12.2000, including provisions on investigations by defence counsel. Under Article 11 thereof, defence counsel or their deputies, authorised private detectives and technical experts must inform the persons they have contacted as they can provide useful information in connection with investigational activities, in line with the relevant provisions of Act n° 675/1996 – i.e., they must specify their capacity and the purposes of the interview as well as whether they are planning to interview them or to hear their statements, and remind them that they are obliged to declare whether they are the subject of investigations or appear as defendants in connection with the relevant or a joint proceeding or else in respect of a related offence, that they may refuse to answer or make a statement and must not disclose the questions, if any, they have been asked by the judicial police and/or the public prosecutor as well as the relevant answers;

d) Legislative decree n° 443 of 28.12.2000, including regulations on administrative documents. Special reference should be made, in this regard, to Article 16(1) thereof, providing that the documents transmitted to other public administrative agencies should only include such data in the special categories mentioned n Articles 22 and 24 of the DPA as concern personal circumstances, events and qualifications that are referred to in laws or regulations and are absolutely necessary for achieving the purposes for which they are collected. Article 78 further stresses that the provisions concerning personal data are left unprejudiced;

e) Ministerial decree of 2 February 2001, concerning the description of types and features and arrangements for installation and use of electronic devices and other technical equipment – so-called "electronic bracelets" – deployed for controlling persons under house arrest/detention, in pursuance of Article 275-bis of the Criminal Procedure Code and Article 47-ter, paragraph 4-bis, of Act n° 354 of 26.07.1975. Article 4 of the above decree regulates the processing of personal data in that it provides that said devices and equipment must be used by respecting the data subject's dignity, the retention period of the relevant data must be limited and the entities authorised to process the data must be specified by also ensuring compliance with the security measures provided for in Article 15 of the DPA.

f) Act n° 135 of 29.03.2001, reforming the laws on tourism; Article 8 thereof provides for amending Article 109 of the Consolidated Public Security Statutes (Royal Decree n° 773 of 18.06.1931) as regards the so-called "hotel cards". Prior to this amendment, the above Article had been modified twice – namely, by Article 16 of Act n° 388/1993, ratifying the Schengen

Agreement, and by decree-law n° 97/1995 as converted into Act n° 203/1995 – in order to bring it into line with the principles laid down in Article 45 of the Convention implementing the Schengen Agreement. Prior to the amendments made by Act n° 135/2001, these cards had to be kept by each accommodation establishment for twelve months and made available to public security officials on request; a copy of the cards had to be transmitted daily to the competent public security department, also via electronic networks. Under the new provision, the manager of each establishment will have to provide the authorities with the identification data of his guests by delivering a copy of the relevant cards; alternatively, he may communicate the identification data included in the cards by computerised or electronic means, in accordance with the mechanisms to be specified in a decree by the Minister for Home Affairs.

Latvia

The Data Protection Law was adopted on 23 March 2000 and came into force on 1 January 2001. The Data Protection authoritiy started work in January this year and its tasks are defined by the above-mentioned law. The European Commission has made some objections in relation to the independent character of this supervisory authority due to its links with the Ministry of Justice.

Latvia ratified Convention 108 on 30 May 2001 and Convention 108 came into force in Latvia on 1 September 2001.

Lithuania

1. General Information

a. The new version of the Law on the Legal Protection of Personal Data, adopted by the Seimas on 17 July 2000, came into force on 1 January 2001. By amendment of the Law on Legal Protection of Personal Data, the Lithuanian legislation is harmonised with EU Directive 95/46/EC. On 20-21 September 2001 there was a meeting of experts from the Council of Europe and the European Commission and the experts of Lithuania in Vilnius concerning the Law on Legal Protection of Personal Data and the Supplementary Draft Amendment. The experts expressed the opinion that the structure and most of the provisions of Lithuanian law on legal protection of personal data follow closely EU Directive 95/46/EC and are in line with Convention ETS 108. The discussions brought out the changes needed to comply with EU requirements. On 31 May 2001 the Supplementary draft of the Law was registered in the Seimas to achieve better co-operation in the justice and home affairs fields with the EU, modified with regard to the opinion expressed by the experts and will shortly be considered by the Seimas. Taking into consideration the comments expressed on the law by the experts, the Law on Legal Protection of Personal Data amendments will be amended to achieve full transposition of the EU requirements by the end of 2002.

b. Furthermore, the Law on ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS N° 108) was adopted by the Seimas on 20 February 2001. On the same date the Seimas authorised the Government to designate an institution to implement the provisions of the Convention. The Convention was ratified on 1 June 2001 and entered into force in Lithuania on 1 October 2001. At present, the Ministry of Foreign Affairs is considering initiating ratification of the Additional Protocol to the Convention ETS 108.

c. The institutional reform of the supervisory institution for personal data protection was executed on 24 September 2001. Following the Law on Legal Protection of Personal Data (in force from 1

January 2001), the Government passed the Resolution under which the State Data Protection Inspectorate is reorganised into an independent governmental institution and will report to the Government from 1 October 2001. The Regulation of the State's Data Protection Inspectorate was adopted by the same resolution. The Inspectorate is designated to implement the provisions of the above-mentioned law as well as of the Convention. Further strengthening of the supervisory institution for personal data protection – the State Data Protection Inspectorate – is envisaged. The Inspectorate is headed by the director, whose term of office is five years and he/she reports to the Prime Minister. The number of staff employees has been increased from 8 to 22. A number of people will be accepted for work in the Inspectorate by competition. In 2002 the Government plans to approve a strategic programme for the development of data protection for 2001 – 2004. At the present this strategy is being prepared and it is hoped that the Government will approve it at the end of this year or at the beginning of 2002. The main objectives of the programme are to establish a reliable and efficient data protection system, which would be in line with EU requirements, to promote the development of technologies enhancing data safety, and to create conditions for electronic public administration and electronic business.

2. Cybercrimes

At the present in Lithuania with Cyber crimes deals Criminal Code of 1961. It has some specific definitions of criminal acts in computer networks, covered by traditional crimes, for example:

- ✓ intentional influence on computer information and its processing (relates to influence on elections or referendum results);
- ✓ fraud (formation of knowingly incorrect computer program, recording of incorrect data in computer memory);
- ✓ damage to property by deception or breach of trust (formation of knowingly incorrect computer program, recording in computer memory of incorrect data).

The new Criminal Code which was adopted in 2000, but not valid yet, has separate section of provisions related to computer crimes – Crimes against informatics:

- ✓ destruction or modification of computer information;
- ✓ destruction or modification of computer program;
- ✓ appropriation and dissemination of computer information.

This new Criminal Code has section of provisions related to the crimes against the inviolability of the person's private life:

- ✓ unlawful collection of information about private person's life;
- ✓ unlawful infringement secrecy of correspondence, telephone conversations, dispatches;
- ✓ unlawful disclosure or use of information about person's private life.

It also should be mentioned that there are present provisions against copyright infringement in this new code, but it will come into force together with new Code of Criminal Procedure.

3. Smart cards

At the present in Seimas one project on Law on the Person Identity Card is registered and is widely considered and discussed.

Present Criminal Code contains provisions dealing with activities such as production, acquisition, storage, realization of false smart cards (credit cards) or illegal disposition of such smart cards, illegal production, acquisition, storage, realization of smart cards. Also these provisions deals with illegal collection or transfer of credit card identification data.

4. Access to official documents

The Law on the Right to receive the information from the state's and local administrations establishes the right for the person to receive information from those institutions and implementation of this right, except when other laws regulate such receiving. The institutions have an obligation to give information about taken activities, the refusal to grant information is allowed when such refusal constitutes a necessary measure in a democratic society and is more important than the person's right to receive information.

The Law on Public Administration provides that at the person's request the entities of public administration must grant him access, in accordance with the procedure laid down in this and other laws, to the documents of public administration adopted by them. The applicant or his representative has the right of access to the available documents and other collected information, also the right to voice his opinion and present additional documents.

The Law on the Constitutional Court establishes that the Court's decisions, resolutions, in some cases, judgments are pronounced publicly in the State's official journal "Valstybės Žinios" (State News), in Seimas special publication, in the newspapers by the Lithuania's Telegram Agency (ELTA).

The Law on the Courts establishes obligation to Ministry of Justice since the 1st of July 2000 to pronounce on the web-site all the effective judgements and resolutions in criminal cases passed by the circuit courts or the Court of Appeal, which have the public interest, the same is with the judgements and resolutions in civil and administrative cases which have the public interest. The resolutions of the Supreme Court are pronounced on the web site.

It needs to be mentioned that the Law on Administrative Proceedings fixes the obligation to pronounce the decision of administrative court for recognition of invalidity of the standard administrative act or it's part.

Malta

The draft data protection law was submitted to Parliament earlier this year and an expert meeting with the Council of Europe and the European Commission was organised in June 2001 in order to examine this draft law. During this expert meeting, some problems in relation to the appointment and dismissal of the data protection authority were identified as well as in relation to the application of data protection principles in the police sector. A draft law in the field of telecommunications is under preparation in order to implement the *acquis* of the EU.

Netherlands

1. On 1 September 2001, the new Data Protection law entered into force, replacing the old one of 1989. The new law implements the EU data protection directive fully and also applies to third pillar matters with the exception of the area that is covered by the existing Police Files Act.

2. By decree of the Queen, many types of processing, precisely circumscribed, are exempted from the duty of notification to the supervisory authority.

3. The law is available in English on the website of the supervisory authority www.cbpweb.nl.

4. The new law obliges us to change our reservations to Convention 108, especially with regard to public registers.

5. The government is preparing a bill on the use of biometry in passports. It is still undecided whether it will be finger print or irisscopy. The purpose of the processing of these biometrical data is to establish whether a passport belongs to the owner. The question arises about what is compatible use. The Parliament asked the government to raise the question with the EU.

6. It is debated in our country whether a general identification duty should be introduced. The events of 11 September 2001 in the US are used as an argument in favour of it. The opponents argue that a general identification duty will be of no use to combat terrorism.

7. Another highly debated issue, also yet unresolved, is the general preservation of traffic data by telecom operators and Internet service providers (ISPs) during a period of 3-6 months. The Article 29 Group of the EU made it clear several times that this measure would be disproportionate and therefore illegal. Police and public prosecutors argue that it is a necessary tool without which much criminality can no longer be traced. The Convention on Cybercrime only obliges the preservation of traffic data in specific cases where a criminal offence is suspected.

EU legislation provides for the deletion of traffic data when no longer necessary for billing purposes but allows exceptions by national law if necessary for the investigation of criminal offences. National regulations might lead though to distortions within the internal market. We are investigating which different categories of traffic data do exist at the moment. Some categories might be more useful to the police than others. In general, preservation of specific categories of traffic data does not affect the protection of private life with regard to other categories.

The problem relates to collected data that must be retained or deleted. We do not aim at the general collection of traffic data by telecom operators or ISPs for police purposes or for state security.

8. The government presented a paper on the echelon-system to Parliament. The paper is available in English. It advocates that countries that intercept communications provide for a legal basis with precise criteria. Citizens of other countries that have reasonable grounds to believe that their basic rights are infringed upon, as they have been intercepted by another country, should have an effective remedy in the sense of Article 13 ECHR in the country from which the infringing measure allegedly originates.

Implicitly it is thus acknowledged that transborder interception might be legitimate.

9. The EU mutual legal assistance agreement of May 2000 (EU-MLA) obliges that consent be asked of the country where the citizen resides whose basic rights are infringed upon. It applies, however, only when the interception is aimed at arresting and prosecuting a criminal. What is said under 8 applies when the EU-MLA does not apply.

Norway

On 1 January 2001 a new Personal Data Act replaced the old 1978 Act; the new act is based on the EU Directive and Convention 108.

In 2000 a report was published on the rights of insurance companies to collect and process data.

Russian Federation

1. On 22 March 2001, the Law on Electronic Digital Signatures was finally introduced in the Russian State Duma. The law was passed by the State Duma at its first reading on 6 June 2001, together with the draft Law on Electronic Commerce. The second reading of the Law on Electronic Commerce and the Law on Electronic Digital Signature is scheduled for October 2001 and after the third reading at the end of 2001, the draft laws are expected to be enforced. The Law on Electronic Digital Signatures is the first law in Russia designed to regulate electronic commerce in the country. Until now, Russian legislation contained few direct or indirect provisions dealing with digital signatures.

The Law on Electronic Digital Signatures defines the rights and obligations of those dealing with digital contracts and digital signatures, and their relationship with state entities in charge of licensing and certification in the area of encrypted information.

The Law also establishes that electronically generated and signed documents are recognized as court evidence.

2. The Law on personal data protection is before the State Duma now.

3. The work in preparation for the signature of Convention ETS No. 108 has been completed following a process of consultations and exchanges of opinion with executive authorities and law-makers. The President of the Russian Federation ordered the Ministry of Foreign Affairs to arrange the signing of Convention 108 in the near future.

Slovak Republic

1. Foreword

In keeping with paragraph 28 (m) of Act N° 52/1998 Coll. on the Protection of Personal Data in Information Systems, the Commissioner for the Protection of Personal Data (the "Commissioner") submitted to the Government and the Parliament of the Slovak Republic a Report on the situation in personal data protection. The Government and the Parliament considered the Report in November and December 2000 respectively. The Parliamentary committee on human rights and minorities took note and expressed its appreciation of the quality of the Report through a resolution in which it recommended that the Commissioner prepare a draft amendment to Act N° 52/1998 Coll. with a view to harmonising the aforesaid Act with Directive 95/46/EC of the European Parliament and of the Council.

The Report is available through the Internet and its hard copies have been provided to all the parties concerned. It has been sent to all partner bodies abroad with known addresses.

2. Fulfilment of the tasks of the State Supervisory Authority for the Protection of Personal Data

The tasks relating to personal data protection are being fulfilled in accordance with the aforesaid Act. Since the beginning of 2001 the State Supervisory Authority has received 34 serious complaints from citizens who claimed breaches of their right to the protection of personal data. At the time of writing this information, 17 of these claims had already been processed. In addition to hearing complaints, the Authority prepared over 200 opinions on the protection of personal data for citizens and public administration bodies.

3. Council of Europe's Convention N° 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

The process of ratification of the Council of Europe's Convention N° 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and Annexes to the Convention has been completed. The Convention entered into force for the Slovak Republic on 1 January 2001.

4. Public information

Because personal data can be given effective protection only if people are aware of their rights, much effort is devoted to providing information to the public. Media are used as the tool for disseminating relevant information material. 50 of such information items were published through printed media, radio and television. The results of public opinion polls, commissioned from a renowned polling agency, indicate that public information about personal data protection increased by more than 15 %. The percentage of Slovak citizens who are aware of their rights concerning the protection of personal data is currently 35%.

5. Draft amendment to Act N° 52/1998 Coll.

The Government of the Slovak Republic charged the Commissioner with the preparation of a draft amendment to Act N° 52/1998 Coll. by 30 June 2001. Given the extensive nature of the amendment, the Commissioner requested that this deadline be prolonged till 30 September 2001. The draft amendment has already been completed and published on the Internet with a view to launching broad public discussion. The amendment is expected to enter into force on 1 January 2002.

Objectives and content of the amendment:

The draft amendment aims chiefly at securing full compatibility with Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive" hereinafter). The second reason for the amendment is to incorporate the comments of experts of the European Commission who examined the situation in the personal data protection area in the Slovak Republic.

The third reason is to make use of several years of experience with practical application of the law which revealed ambiguities in its current wording, and to eliminate them with a view too increasing legislative and technical clarity of the law and, naturally, ensuring better harmony with legal provisions that entered into effect in the recent period. They include, for example, Act N° 211/2000 Coll. on Free Access to Information and on amending and supplementing certain other laws. It became clear that the definition of certain terms should include the concepts of "access to personal data" and "publication of personal data". Recent research on biometrical data has demonstrated the need to deal with such new areas of knowledge as DNA analysis, which have a significant impact on the processing of personal data. The processing of biometrical data thus constitutes a special and independent category of personal data. New paragraph 4 provides that biometrical data can be processed only under conditions set out in separate law. The processor may process biometrical data only if this is expressly provided for in the legislation, or subject to a written consent of data subjects. An exception is provided for under paragraph 5 where biometrical data (such as fingerprints) are used as identifiers to authorise entry to premises. In this case the processor is not required to obtain permission to process biometrical data under a separate law; however, he may not process the data without the consent of data subjects whose consent may not be forced.

The law must precisely define conditions under which no consent of data subjects is required. In processing personal data, data processors are deemed to have obtained the consent of data subjects where the persons concerned did not explicitly raise objections thereto. Inspections revealed a number of irregularities in this respect. Many ambiguities were detected also in connection with the type of

personal data that the processors may request from persons seeking one-off access to premises. The proposed draft provides also for this area.

Substantial changes are proposed in respect of the registration of information systems. These changes are of organisational and substantive nature. The most essential change consists in assigning the responsibility for registration to the State Supervisory Authority for Personal Data. All relevant activities are thus logically performed by a single organisational entity. The existing division between two central state administration authorities (Statistical Office of the Slovak Republic and Government Office of the Slovak Republic) is unusual in Europe.

The amendment section that deals with the State Supervisory Authority for the Protection of Personal Data contains provisions that will increase independence of this authority. This complies with the requirements of the Directive and with the demands expressed by the European Commission at each examination. Independence of the Authority should be enhanced through the proposed procedure of appointing and recalling the commissioner. This procedure is in harmony with those applied in the countries that have presidents as the heads of state. The amendment proposes the creation of an advisory and appellate body for the commissioner, ie the Council on the Protection of Personal Data. The Council should give opinions on all complicated questions relating to the protection of personal data. The creation of a similar advisory body is common practice in the countries where the office of State Supervisory Authority is held by a single person rather than a commission. The change in the status of employees of the authority supervising personal data protection and the structure consisting of deputy commissioner, inspectors and other employees, reflect both the requirement of the EC expert mission and practical experience obtained during inspections of the processors of data. It has become clear that the deputy commissioner and inspectors must be granted the status of public officials.

The amount of fines was brought in line with the fines imposed in neighbouring countries. The upper threshold of fines imposed for the beach of personal data protection legislation in EU countries is equivalent to around SKK 7 million. We propose to set the fine at SKK 10 million. The amendment contains also a change in the power to impose the fines, vesting it directly in the State Supervisory Authority for the Protection of Personal Data. The decision to impose a fine may be appealed against. Appeals will be heard by the Council on the Protection of Personal Data.

After the coming into effect of Act N° 52/1998 Coll., the protection of personal data in the Slovak Republic may be deemed to be fully comparable with the protection provided in EU countries.

Slovenia

In 2000 an amendment to the data protection legislation was introduced in order to establish an independent data protection authority.

Spain

The data protection law of 1992 was revised in 1999 following several judgments of the Spanish Constitutional Court and has been underpinned by several regulations: (1) on international data transfers to ensure compliance with the legislation; (2) security regulations of 11 June 1999. Under these security regulations it is not only necessary to say that security measures must be taken to ensure an adequate level of protection, but there must also be a minimum level of technical measures to prevent misuse of the data.

Three recent decisions by the Spanish Constitutional Court regarding data protection as a fundamental right of citizens will have important consequences in the legal system because it will imply more jurisdictional guarantees.

Legislation on electronic signatures was adopted on 17 November 1999.

Regulations on video surveillance were passed in 1997 in connection with terrorism problems.

Sweden

The Swedish Personal Data Act entered into force on 24 October 1998 with a transitional period. The transitional period for automated processing of personal data has now come to an end. This means that the Personal Data Act entered fully into force on 1 October of this year (2001) as concerns automated processing of personal data. Sweden continues to implement and adjust other legislation that concerns processing of personal data in order to bring it into conformity with the EU Directive, Convention 108 and the Swedish Personal Data Act. The Government has taken a decision on the implementation of the Commission of the European Communities Decision of 15 June 2001 on contractual clauses for the transfer of personal data to third countries. This means modification of the provisions of the Personal Data Ordinance that will enter into force on 1 December of this year (2001).

Suisse

Depuis notre dernière réunion, des travaux en vue d'une révision partielle de la loi fédérale du 19 juin 1992 sur la protection des données ont débuté. Le gouvernement a mis en consultation un avant-projet de loi, que vous pouvez consulter sur notre site internet (www.edsb.ch). Ce projet fait suite à deux motions parlementaires et doit permettre à la Suisse de ratifier rapidement le protocole additionnel à la Convention 108. Les principales innovations du projet sont :

- renforcement de la transparence avec l'obligation d'informer les personnes concernées lors de la collecte de données sensibles ou de profils de la personnalité. En outre la collecte doit être reconnaissable pour tout type de données ;
- devoir d'information également lors de la prise de décision sur le seul fondement d'un traitement automatisé ;
- abandon de l'obligation de l'annonce des fichiers dans le secteur privé ;
- modification du régime des flux transfrontières : abandon du régime de la déclaration préalable et rapprochement avec le système du directive européenne : pas de transfert en l'absence de niveau adéquat. Le transfert est possible, dans un cas d'espèce, lorsque certaines conditions sont remplies.
- Amélioration de la position de la personne concernée lorsqu'elle s'oppose au traitement des données la concernant par une personne privée ;
- Introduction d'une base légale pour les projets pilotes avant l'entrée en vigueur d'une base légale formelle autorisant un tel traitement et renforcement des exigences et des possibilités de contrôle lors du traitement de données fédérales par des organes cantonaux, en exécution du droit fédéral.
- Introduction du droit de recours du Préposé fédéral à la protection des données contre les décisions de la Chancellerie ou des départements rejetant ses recommandations.

Ce projet ne constitue pas encore une transposition de la directive européenne. Le Préposé fédéral à la protection des données, qui a été associé à la révision, soutient dans son ensemble le projet. Toutefois,

il regrette que cette révision ne soit pas plus ambitieuse et que l'occasion n'ait pas été saisie de procéder à une modernisation du droit de la protection des données.

Un autre projet de loi sur la transparence de l'administration sera transmis au Parlement cette année encore. Ce projet confère en particulier au Préposé fédéral à la protection des données des tâches de médiation en cas de conflit entre l'administration et un particulier, non seulement lors d'une demande d'accès à des données personnelles, mais également à d'autres documents administratifs. L'accès aux données personnelles d'un tiers est régi par la loi fédérale sur la protection des données. La règle est que les documents administratifs doivent être anonymisés avant d'être communiqués. Lorsque cela n'est pas possible, l'accès sera notamment possible exceptionnellement si la divulgation dans un cas d'espèce est justifiée par un intérêt public prépondérant. La personne concernée pourra être entendue si elle en fait la demande. Son avis sera en tous les cas recherché lorsque la demande porte sur des données sensibles ou des profils de la personnalité. Dans ce cas, l'opposition de la personne concernée entraine le rejet de la demande d'accès.

Le gouvernement a également adressé au Parlement un projet de loi en vue de la ratification de la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine.

Pour sa part le Préposé fédéral à la protection des données a publié son 8e rapport d'activités. Nous avons également publié différents documents d'informations dont :

- un guide relatif à la surveillance de l'internet et du courrier électronique au lieu de travail ;
- un aide mémoire sur la vidéosurveillance effectuées par des personnes privées.

Ces informations sont également disponibles sur notre site internet www.edsb.ch.

Enfin depuis le 1er septembre 2001, Monsieur Hanspeter Thuer, avocat et ancien conseiller national, est devenu le nouveau préposé fédéral à la protection des données en remplacement de Monsieur Odilo Guntern qui a pris sa retraite.

"the Former Yugoslav Republic of Macedonia"

In September 2000, the Government decided to bring several laws up to date, including a new Law for the Protection of Personal Data (the previous law dates from March 1994), in order to provide a higher level of protection of personal data, to follow the standards and criteria established by international legal instruments, to harmonise the law with the legislation in the old democratic countries and to correspond with the new technologies implemented in everyday living.

The project group was instructed to prepare a new version of the Law by the end of 2000. The first version was finished and sent to Governmental institutions and the academic community for their opinion. The answers came in with different notices for improvement of the text.

The main plan of the group was to include in one package the ratification of Convention 108 and the Law for the protection of personal data, for acceptance by Parliament. Given the instability of the current political climate, the whole process was stopped.

However, the project group is determined to place the Convention and the Law on the Parliament's schedule as soon as possible, considering the current activities on changing of some articles in the Constitution.

Neglecting the present situation, it is necessary to stress the background of the Law:

1. The protection of data is provided by the Constitution in Article 18, which declares that "the State guarantees the security and the secrecy of personal data". In the second paragraph of this

Article "everyone is entitled to legal protection of his personal integrity related to registering and processing the personal data".

2. The rights of the citizens on security and secrecy of personal data are regulated by the Law for the protection of personal data (Official Gazette N° 12 of 1994).
3. In practice, the existing Law showed weaknesses in the protection of personal data as well as a protection of personal integrity, which is related to the processing of data. Moreover, it does not correspond with the standards and criteria for the protection of personal data already established in relevant international legal instruments and with the legislation in countries with developed democracy.
4. The concept of civil society and establishing of fundamental freedoms and rights of citizens has been accepted as a basic value of the State.
5. The will of the State to be a full member of the EU produces a need for harmonisation of the Laws with international legal progress and shaping relations in all spheres of everyday living, including the protection of personal data.
6. "the former Yugoslav Republic of Macedonia" was the first country to sign the Pact for Stabilisation and Association and committed to harmonising the laws in accordance with the EU legislation. One of the first steps regarding data protection was to establish a common information system on the national level for border control of the flow of personal data.

The Law is based on the following principles:

1. Legality and fairness in personal data processing
2. Definition of the purpose for the setting-up of a database
3. Data subjects should give agreement for processing of their personal data
4. Data subjects should have free access to the database
5. Controllers and operators (administrators) should be responsible for handling the data base
6. Sensitive data should be subject to special protection
7. There should be controlled links between databases containing personal data
8. Transfer of data across borders.

Reform of Payment system

The competition in the market economy has evolved in many fields except in the payment system. The Bureau for Payment Operations had a monopoly on payment operations which was an obstacle to the improvement of the financial system and in the strengthening of the economy.

To change the monopoly of the BPO and to induce competition between banks, the State started to work on a reform of the payment system.

The new system is based on business relations between banks and their clients – the owners of the accounts. The goal is to spread the financial services, reduce the price of services and introduce new offers, focusing on supplying credits.

There are two ways of payment, either through the Macedonian Interbank Payment System (MIPS) or the Clearing Interbank System (CIBS) or Clearing House, depending on the amount of money.

Some of the banks are preparing for the electronic payment from home. By the end of the year, the Ministry of Finance will bring final necessary regulations to provide e-banking and e-commerce.

It is expected that in parallel with the finalisation of the regulation, a national card for payment should be involved in banking operations. From the technical aspect, it will produce installation of autonomous switching centre(s) for processing and collecting data in the field of smart cards.

Turkey

No developments. The draft data protection law is still under examination.

United Kingdom

Freedom of Information

In November 2000, the Freedom of Information Act 2000 was passed. (This Law does not apply to Scotland which has a separate law). Most of the Act's provisions are not yet in force. They must be implemented by November 2005. The Government has not yet announced the timetable. The Act gives the former Data Protection Commissioner responsibility for overseeing the new legislation, and renames her the Information Commissioner. Similarly, the former Data Protection Tribunal is renamed the Information Tribunal. These changes are already in force.

National Security

On 1 October 2001, the Information Tribunal announced its Decision on an appeal under the Data Protection Act 1998. The appeal was against a certificate issued by the Home Secretary which the Security Service relied on in refusing a subject access request on grounds of national security. The Tribunal quashed the certificate. The main ground was that the certificate was too general: it allowed the Security Service to claim the exemption evening cases where national security was not an issue. This Decision does not mean that the national security exemption no longer applies. Its effect is that the Security Service can no longer rely on the certificate as evidence of the need for the exemption. It is open to the Home Secretary to issue a differently worded certificate.

Administrative changes

In June 2001, responsibility for policy on data protection and freedom of information passed from the Home Office to the Lord Chancellor's Department.