COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 18 June 2012

T-PD(2012)02Mos
Addendum

**CONSULTATIVE COMMITTE OF THE CONVENTION
FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING
OF PERSONAL DATA
(T-PD)**

**LE COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES
PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ
DES DONNÉES A CARACTÈRE PERSONNEL
(T-PD)**

Information on the recent developments at national level in the data protection field

Information sur les développements récents intervenus dans le domaine de la protection des données au niveau national

DG I – Human Rights and Rule of Law / Droits de l'Homme et État de droit

TABLE OF CONTENTS

CROATIA / *CROATIE*

REPUBLIC OF CROATIA
Agency for Protection of Personal Data
Zagreb, Martićeva 14
Klasa: 910-01/12-01/34
Urbroj: 567-04/05-12-01
Zagreb,31st of May 2012

COUNCIL OF EUROPE
SECRETARIAT GENERAL
Directorate General

Human Rights and Rule of Law
Information Society and Action Against Crime

DIRECTORATE
DATA PROTECTION AND CYBERCRIME
(via e-mail: szilvia.simond@coe.int)

Requested quote: DGI/AS/SK/cg

Subject: Consultative Committee of the Convention for the Protection of Individual with Regard to Automatic Processing of Personal Data (T-PD).

Dear Sir/Madam,

According to your request, in the continuation you can find the Report on the Activities of the Croatian Agency for Protection of Personal Data for the period between December 1st 2011 and May 25th 2012. The mentioned report was requested in order to be included in the compilation of the materials for the upcoming T-PD Plenary Meeting in Strasbourg between June 19th and June 22nd 2012.

I. PERSONAL DATA PROTECTION

LAW AMENDMENTS

Since the Amendments to the Personal Data Protection Act (Official Gazette No. 130 of 11/16/2011, which entered into force on 11/24/2011) were adopted, the provisions of the Personal Data Protection Act are in its totality in accordance with the Directive 95/46/EC.

PROJECTS

During the reported period the Agency has participated in the next projects:

1. IPA 2007 Twinning project "Capacity Building of the Croatian Agency for Protection of Personal Data" (HR/2007/IB/JH/02)

- The 2nd Annex of the project was signed which extends the project for 2 extra months and foresees its culmination the July 28th 2012. New activities were incorporated to the project: programme for raising awareness of data protection officers, supply of advertising material and production of advertising spot.
- Held the workshop “Data Protection and Free Access to Information in the Croatian Legal Framework” where the target group were the courts administration.
- Organized and trained a special unit in the Ministry of Internal Affairs dedicated to the personal data protection in that ministry (over 600 attendants).
- Defined the procedures related to ISO 27001 standards for information security.

We can conclude that already now the results of this IPA 2007 Twinning project are even above the first expectations.

2. ”Enhancing capacities of the CAPPD in the field of right of access to information” - project within the framework of the Dutch pre-accession bilateral assistance programme.
    - Analysis of the current legal frame and its compliance with the EU legislation.

3. „Improving the Access to Information in Public Administration“- project within FFRAC 2010 and expecting for the EUD authorization, however, due to possible changes in the related legislation a postponement was recommended.

4. „Strengthen the Implementation of the New Freedom of Information Act“ - project within the framework of DIV/Reuniting Europe Programme
    - 3 workshops were held dedicated to the information officers.

5. "Perception of the Data Protection and Privacy Issues by Children and Youth" - project held in the Leonardo da Vinci Programme framework
    - A survey was organized among 6th grade elementary school, and 2nd grade high school children, on personal data protection perception and children and youth on-line privacy.
    - A termination of the programme was requested due to Hungarian partner renounced to the project.

    Although the project was terminated before it was foreseen, the Agency has made the complete analysis of the leaded survey and this way fulfilled the predicted goals. The analysis of the result will be used for future activities related to child privacy protection.

6. „Strengthening the Role of Youth in Democratic Civil Society“- project which was applied to the UNDEF (The United Nation Democracy Fund) tender.

7. TAIEX assistance:
    - study visit to the Slovenian Information Commissioner,
    - study visit to the German Personal Data Protection Agency
    - workshop "Balance between the Right of Free Access to Public Information and Personal Data Protection in Media Reporting "
    - approved the visit of public interest and proportionality test expert

8. In the framework of the Lifelong Learning Programme Leonardo da Vinci, the Agency on 2012 together with its partners from Bulgaria, Czech Republic and Poland, apply to the project "Raising Awareness of the Data Protection Issues among the Employees Working in the EU"

INFORMATION SAFETY

- The Agency carried out the needed preparation activities for introducing Security Zone II, in compliance with the provisions of the Information Safety Act (Official Gazette 79/07)
- The Agency completed the activities to receive the ISO 27001 Certificate, understanding by that the incorporation of a administration system for information security. The certification of the Agency would indicate that it's ready for the execution, administration, control, keeping and improving a documented ISMS within the Agency's labour activities

SUPERVISION

In the reported period the Agency has acted *ex officio* as well as according with the submitted requests for personal data protection

In this six-month period 126 data protection requests have been submitted to the Agency. The majority of them were related to: on-line personal data processing (web forums and sites, social networks, etc.), personal data processing with marketing purposes, legal acts execution and legal assignment, transfer of personal data, processing of personal data on association membership, and others.

Among the totality of the submitted protection requests, 44 were related to personal data processed by *Imenik d.o.o.*, a trade association from Zagreb, on its web site www.imenik.hr. The submitters remarked that there was publicly published the personal data of trade associations legal representatives without any legal basis. The same trade association was accused for publishing all the subscribed public telephone numbers in Croatia. Smaller number of requests was related the processing of hidden telephone numbers in the abovementioned website.

In the mentioned case, the Agency determined that the personal data of the trade association legal representatives was processed and published without legal basis and in discordance with the Personal Data Protection Act. Therefore, the Agency has forbidden *Imenik d.o.o.* such personal data processing and requested the deletion of the embraced personal data. Also, the Agency found the processing of the prepaid telephone numbers and related personal data in compliance with the Croatian Telecommunication Act. The Agency is still deducing if the secrecy of the hidden numbers was properly requested.

A certain number of personal data protection requests were submitted due to on-line publishing of personal data (social networks included), in such cases data deletion was requested by the submitters. However, in the cases when the domain is located outside Croatia, this Agency hasn't authority for such action.

It's important to remark the increasing number of requests for personal data protection regarding the marketing offers of insurance companies, prize game participation and association membership.

In the *ex officio* held cases and supervision of records delivery to the Central Register, the Agency requested to Personal Data Filing System Controller the delivery of records, and correction of the already delivered ones, in accordance with the legal provisions.

In the period this report refers to, the Agency enacted 5 decisions acting *ex officio* against Personal Data Filing System Controller, and 15 decisions and 32 opinions acting by the submitted requests.

According with the national laws, the decisions of this Agency can be revoked only by administrative complaint to the Administrational Court. In this period 4 of such processes have been started against Agency decisions, and that processes are still continuing. Also, the Administrational Court dismissed one complaint against an Agency decision.

Finally, the Agency has started 2 processes against Personal Data Filing System Controller and the responsible person at the Misdemeanour Court.

CENTRAL REGISTER

Personal Data Filing System Controller and Recorded Personal Data Filing Systems

From the next tables is appreciable the number of Personal Data Filing System Controllers and Records on Personal Data Filing Systems that have been recorded during the reported period, as well as the total figure.

Personal Data Filing System Controller

Status on 11/30/2011	Period	New Records	Total no. of Records till 05/18/2012
7.811	12/1/2011 05/18/2012.	476	8.287

Records on Personal Data Filing Systems

Status on 11/30/2011	Period	New Records	Total no. of Records till 05/18/2012
18.005	12/1/2011 05/18/2012.	1.602	19.607

PUBLIC RELATIONS, EVENTS AND SEMINARS FOR PDFS CONTROLLERS

Cooperation with Media

The Agency answered the enquiries frequently and reported timely throughout all the public information means: interviews, written answers, press releases as well as through its website. It's important to remark that the Agency answered press enquiries or held media presentations of the Agency's work 24 times.

Events and Seminars

Date	Activity	Target Group
01/26/2012	Seminar and Workshop Zagreb	PDFS Controllers
01/26/2012	„Open Doors Day“	Public
01/26/2012	Lecture „Privacy Protection and Free Access to Information in the Work with the Media“	Studenti VŠ „Kairos“
01/27/2012	Lecture and Additional Programme „Privacy Protection of Children“	Elem. School Matka Laginje
02/07/2012	Info-Point - Safe-Internet Day	Public, especially children
03/13/2012	Seminar and Workshop Slavonski Brod	PDFS Controllers
03/14/2012	Seminar and Workshop Sisak	PDFS Controllers
03/15/2012	Seminar and Workshop Karlovac	PDFS Controllers
05/09/2012	Workshop „Young Personal Data Filing System Controller“	Elem. School Matka Laginje

II. RIGHT OF ACCESS TO INFORMATION

In relation with the access to information right in this six-month period, the Agency has received 260 cases and has started 4 misdemeanour processes before the relevant court in compliance with the article 26th of the Right of Access to Information Act.

The Agency participated in the Partnership for Open Governance initiative for making an Action Plan. In the framework of the project „Strengthen the implementation of the new Freedom of Information Act“, the Agency actively took part of 5 workshops for information officers. The Agency has also organized, in cooperation with TAIEX, a workshop on “Balance between the Right of Free Access to Public Information and Personal Data Protection in Media Reporting“. With the support of TAIEX the Agency employees had a study visit to the Slovenian Information Commissioner on “Specific Topics Related to the Right of Access to Information in Public Administration”. Also, the Matra Flex project has started on the topic „Enhancing Capacities of the CAPPD in the Field of Right of Access to Information”.

The Report on the application of the Right of Access to Information Act for the year 2011 was composed, as well as the Report on Forming and Conducting the Overview of Signed and Executed Public Tender Contracts.

Finally, the since April 2012 the Agency is participating in the Working Group for Amending the Right of Access to Information Act.

Sincerely yours,

DIRECTOR

Dubravko Bilić, mag.philol.croat**.**

Addressed to: Data Protection and Cybercrime Directorate

Copy: Archive of the Croatian Agency for Protection of Personal Data

CZECH REPUBLIC / *RÉPUBLIQUE TCHÈQUE*

úřad pro ochranu osobních údajů
the office for personal data protection

MODERNISATION OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS NO. 108]

Text after 27th T-PD meeting - 27 April 2012

Proposals for amendments Czech Republic
May 2012

Generally

Although the Czech Republic has already presented some proposals for amendments at the T-PD meetings, for the sake of clarity they are included in this text. The proposals follow Guideline 18 of the Joint Practical Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of legislation within the Community institutions[1] and also Chapter II.IV of the Manual of Precedents for acts established within the Council of the European Union.[2]

Proposals for amendments

1. In Article 2 letter c shall be replaced by the following:
   "c. "data processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction; if personal data are generated either through automated means or by intellectual effort, then such operation means processing;"

Explanatory note:

The term "collection" undoubtedly covers the beginning of the processing of personal data and the very moment from which the regulation should apply—for processing based on collection of personal data from data subjects or receiving already existing data from another controller or someone else. Such a situation—as far the applicability of the regulation is concerned—is clear. Unclear is the starting moment for the applicability when personal data are created by whom is carrying out the further processing, especially by technical means' performance—such as video surveillance systems, smart devices systems using sensing applications, geolocation, usage-based billing, access control and advance monitoring in general.

Clear reference to, and absolute clarity of, the concept of processing is crucial for the implementation of the Convention, especially supervision. It is of the same importance for subjects responsible pro processing or taking part in it.

2. In Article 5(2)(a) the word "explicit" shall be replaced by "provable".

[1] http://eur-lex.europa.eu/en/techleg/index.htm
[2] http://ec.europa.eu/translation/documents/council/manual_precedents_acts_en.pdf

Explanatory note:

Implicit consents shall be also considered as valid. Almost every contract includes a lot of personal data; it is of no usefulness to enumerate them explicitly. Instead, the capability of being demonstrated or logically proved is essential; the form which it takes may vary depending on technology or means of processing. This change also provides for technological neutrality and addresses another key characteristics of the data subject's consent—that the consent must be proved later.

3. In Article 5(2)(a), the words "specific and" shall be deleted.

Explanatory note:

See above.

4. In Article 5(2)(b), the words "or contractual obligations binding the data subject" shall be deleted.

Explanatory note:

The Convention 108 distinguishes between "consent" and "contract". But every bilateral contract consists basically of two parties' consents together. So does a "consent" which is within the meaning of the Convention 108 bilateral legal negotiation between a data subject who gives consent and a data controller who accepts it. Therefore this artificial difference should be abandoned.

5. The following words shall be added to Article 5(3) (d): "personal data established as inaccurate shall not be disclosed unless rectified or marked appropriately".

Explanatory note:

The provision is inadequate. There is a need to provide for the quality in situations when personal data are to be transferred, more precisely to prevent controllers and processors from transferring personal data of the known inaccuracy.

6. The following letter shall be added to Article 5(3):
   "(f) lawfully published personal data".

Explanatory note:

Republishing is legitimate purpose of data processing. Art. 5(1) has no meaning there. Although Art. 5(2) (b) puts a space for domestic legislation, it is better to put it there expressly.

7. The following paragraph shall be added to Article 6:
   "3. Processing of data relating to criminal convictions or related security measures may be carried out either under the control of the public authority or when processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by the Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only by the public authority."

Explanatory note:

Sensitive data processing nature is relative. Some sensitive data in some context are not sensitive at all and vice versa.

8. The following paragraph shall be added to Article 6:
   "4. Conditions set up in paragraph 1 shall apply for processing of any set of personal data including unique identification data together with any data concerning private life of data subject."

Explanatory note:

Sets or combinations of personal data generally perceived as directed at data subject's vulnerability are made subject to stricter rules.

9. Article 9(1)(a) shall be replaced by the following:
   "a. protect national security, public order, the national economic and financial interest or the suppression of criminal offences".

Explanatory note:

Standard preventive measures consist of national security and public order. Since this wording is traditional, specification: "when such derogation is provided for by law" has no meaning there.

It could not be agreed on the prevention of criminal offences inclusion, since this is misused for lowering of human rights, especially privacy an human dignity by CCTV, exploring DNA etc.

10. Article 25 is **under question**:

Explanatory note:

Is Art.19–23 of the Vienna Convention on the Law of Treaties applicable to the Convention 108? The important decision concerning the mentioned problem should be taken. In case the Vienna Convention on the Law Treaties is applicable, Art. 25 of the Convention 108 should be deleted.

úřad pro ochranu
osobních údajů
the office for personal
data protection

Czech Republic
Office for Personal Data Protection
Information on the major developments in the data protection field in 2011

- In 2011 the Office applayed in very concentrated way its supervisory powers on illegal video surveillance running within the meaning of the Act on the Protection of Personal Data.

- As a result of these Office's activities the situation in monitoring in the towns and transport was improved. Video surveillance using was strengthened in limits and on the basis of special laws.

- The Labor Code is primarily violated by the employers who monitor using video surveillance the employees in their workplace. That is why the Office iniciated and has developed the cooperation with the labor inspectorates.

- As for video surveillance running in the residential buildings the Office elaborated the recommendation for housing cooperatives and residentional units owners.

- In connection with developing of the Action Plan originated from the Government Resolution of September 14th 2011, which was adopted in context with an international initiative Open Government Partership, the Office has actively participated in all negotiations coordinated by the Deputy Prime Minister and enforced essential amendment to the Act on free access to information with the aim to clarify the links to the Act on the Protection of Personal Data.

- In various contacts with the mass media staff the Office spread the knowledge of the Act on the Protection of Personal Data among the journalists and debated with them specific cases of its application in their work. Both sides, the Office and mass media representatives, expressed the interest to continue in this cooperation.

- In cooperation with the Polish supervisory authority (Biuro Generalnego Inspektora Ochrony Danych Osobowych) and Hungarian supervisory authority (Adatvédelmi Biztos, Parliamentary Commissioner for Data Proteciton and Freedom of Information) was established a publication – an aid for personal data controllers „Selected data protection issues. Guide for interpreneurs", supported by the European Lifelong Learning Programme Leonardo da Vinci (Education and Culture DG), which was published in Polish, Hungarian, English and Czech in 2011.

- In 2011 the yearly held competition for youth „My Privacy! Dont' look, dont' poke about!" was focuded on propagation of knowledge of problems connected with the use of Social Network, which threatens the privacy of its users.

FINLAND / *FINLANDE*

14.6.2012

INFORMATION ON THE MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD IN FINLAND SINCE THE 27th PLENARY MEETING OF THE T-PD

The Parliament of Finland approved the 2001 protocol ETS No.181 and the required national law for incorporating the provisions into national law on 27 March 2012. Both instruments will be presented to the President of the Republic for approval and confirmation respectively in late June 2012.

The action of the Data Protection Ombudsman

1. Data Protection Day

The Data Protection Ombudsman did run a workshop on the theme of "What's coming about in the security breach?", in which was discussed about the potential risk of security breach to the citizens in reality, do we have right tools to react to it?

The Data Protection Ombudsman did also stage a press conference about the discovery of the workshop and allowed for discussion and questions concerning it and protection of personal data in general.

He also made on hand the material of data protection to children and the youth in the virtual Habbo Hotell.

2. The other action

The main emphasis in the action of the Data Protection Ombudsman has still been, in accordance with his goals, preventive operations. Aiming to have an influence on the public, he has focused on giving appropriate advice and guidance and integrating into working groups and committees which are significant in the field of data protection.

The office of the Data Protection Ombudsman has still had extensive co-operation with different interest groups. Various data protection steering groups has been operated in, among others, the sectors of public health care, social welfare, telecommunications and education.

GERMANY / *ALLEMAGNE*

07 June 2012

Developments in the field of data protection at national level in 2011/2012
Germany

1. German Bundestag Study Commission on the Internet and Digital Society
In 2010, the German Bundestag decided to set up a study commission to look at the Internet and the digital society. 17 Members of Parliament and 17 experts have combined their efforts to study the issues in hand and are expected to submit their findings and recommendations by March 2013.
So far, the study commission has concluded four project groups. These are the project groups on data protection, media literacy, net neutrality and copyright. Further project groups are currently active, these being the ones dealing with democracy and the state, business, labour affairs and green IT, online access, structure and security, education and research.
The project groups dealing with interoperability, standards, open source; culture, the media and the public; international issues and internet governance and consumer protection are expected to take up work in June 2012.

The following interim reports and policy recommendations have so far been published:

- Interim Report on Data Protection and Privacy Rights ("Zwischenbericht zum Thema Datenschutz und Persönlichkeitsrechte") (15 March 2012)
- Interim Report on Net Neutrality ("Zwischenbericht zum Thema Netzneutralität") (2 February 2012)
- Interim Report on Copyright ("Zwischenbericht zum Thema Urheberrecht") (23 November 2011)
- Interim Report on Media Literacy ("Zwischenbericht zum Thema Medienkompetenz") (21 October 2011).

For further information - in the German language - concerning the study commission and the interim reports compiled by it please go to
http://www.bundestag.de/internetenquete/index.jsp

2. Federal Government internet policy
The Federal Ministry of the Interior discussed the future of German internet policy with representatives from civil society, industry, research and administration during four consultations in 2010.
Discussions have focused on the issues of data protection and data security and have been summed up in 14 theses on internet policy to be found at http://www.bmi.bund.de The Federal Ministry of the Interior has taken various measures to implement these internet policy recommendations; it has, for instance, launched the Code for Social Networks, which is currently being drawn up.
In November 2011, the internet industry, at the initiative of the Interior Ministry, began to draw up pragmatic rules to protect users and consumers in social networks, led by the Voluntary Self-Regulation Body of Multi-Media Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, FSM), an organization which has already gathered practical experience with voluntary commitments.
The following enterprises take part: Facebook, Google, LinkedIn, Lokalisten, StayFriends, VZ Netzwerke, wer-kennt-wen.de and XING AG. This means that the most relevant national and international providers have been enlisted.
The Federal Government supports the efforts to elaborate the above-mentioned code, which is expected to be finalized in the last six months of 2012. The participating companies and the FSM have agreed to lay down voluntary commitments regarding i.a. the following issues:

- privacy by default
- data security
- transparency and controls for users
- concerns of younger users
- adequate risk management, e.g. efficient ways to report inadequate content
- user-friendly log-off processes and ways to delete user data
- right of non-users to determine the use of their data
- transparency with regard to the data stored.

3. Contest "Vergessen im Internet" (Forgetting and the Internet)
On 7 May 2012, the Federal Minister of the Interior, together with the German Academy for Technical Sciences (acatech; Deutsche Akademie der Technikwissenschaften), selected the winners of the contest launched in April 2011 to gather ideas on how to limit the shelf-life of internet content.
Pupils, students, businesses and private individuals had been invited to submit contributions in the three categories of "making users aware of risks", "manners and rules", and "technical forgetting solutions".

4. Draft Act to Regulate Data Protection in the Employment Sector
On 25 August 2010, the Federal Government adopted a Draft Act to Regulate Data Protection in the Employment Sector, which is currently going through the parliamentary process. This process is accompanied by a broad discussion by business and academia, interest groups and the general public.

5. Data Protection Foundation
The Federal Government is planning to set up a data protection foundation, which is

- to look at whether products and services comply with data protection needs,
- to enhance data protection education,
- to make users more aware of data protection measures which they can take to protect their data and
- to develop a data protection audit.

The plan is to set up the foundation as a non–profit and incorporated entity under public law. A total of 10 million euro has been earmarked for the foundation’s assets in the federal budget.

Policy discussions are currently being held concerning the establishment of the Data Protection Foundation.

6. DE-Mail Act
On 3 May 2011 the Federal Government adopted an Act called “DE-Mail Act”, DE being short for Deutschland, or Germany.
The Act seeks to make important security functions for the electronic exchange of messages user-friendly and thus accessible to a broad general public.These functions are, among other things, encryption, verifying the identity of communication partners, and making it possible to prove that a message has been sent or received – functions not available under the current mailing systems.
The new provisions and the technical guidelines governing DE-Mail have created the necessary framework conditions. DE-Mail has been realized and operated by accredited, mostly private, providers.
Potential DE-Mail providers may apply to the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to be approved for the above-mentioned services. So far, Deutsche Telekom AG, United Internet (which provides web.de

and GMX), Deutsche Post AG and the Mentana Claimsoft company have announced that they intend to provide De-Mail services.

7. The electronic identity card

On 1 November 2010, the new electronic identity card was launched in Germany. It enables card holders to prove their identity - safely and unequivocally – when using the internet or toll machines and other technical devices. The ID card chip can transmit the necessary data using secure connections as soon as the card holder authorizes such transmission by entering a PIN. Authorization certificates control which personal data may be transmitted to providers of internet applications and administrative services.

The Federal Commissioner for Data Protection and Freedom of Information was involved in the process of designing the new personal identity card from an early stage, and has acknowledged that it is privacy-friendly. Privacy-by-design played an important role. The EAC, BAC and PACE protection mechanisms, which have been applied in this context, are recognized world-wide in terms of data protection and rank top under IT security aspects.

Data stored on the new identity card can also be secured by what is known as “authorization certificates”. To this effect, the “authority issuing authorisation certificates” (Vergabestelle für Berechtigungszertifikate, VfB), has been set up at the Federal Administration Office. Any enteprise, institution or authority wishing to access ID card data has to apply for the corresponding access rights. This authority will then check thoroughly whether or not applicants actually need the data for their business transactions. If not, authorization will be denied.

The federal Länder are responsible for making specific arrangements in order to manage the tasks arising from the law governing ID cards. This means that the identity card authorities must take measures to ensure the protection of personal data held or used by local authorities. That said, the Federal Ministry of the Interior makes every effort to assist these authorities and has given them IT security guidelines developed by the Federal Office for Information Security especially tailored to their needs.

8. Amendment of the Telecommunications Act

On 10 May 2011, the Act to Amend the Telecommunications Act entered into force. The aim is to adopt new information and transparency rules (for instance regarding the location of persons) and to thus improve data protection provisions. The overarching aim is to better protect sensitive data and to strengthen the legal position of those using telecommunication services.

9. Cloud computing

The Federal Ministry of Economics and Technology has launched a technology programme called “Trusted Cloud”. In the next three years, 14 innovative, secure and legally robust cloud solutions will be developed and tried in various application fields. At the same time, the Ministry of Economics has set up the “Trusted Cloud Competence Centre”, which brings together several working groups to address cross-cutting issues. The working groups are coordinated and accompanied by experts. One working group deals with the legal framework concerning cloud computing (including data protection).

10. IT summit

The mobile internet entails additional data protection challenges e.g. because it can easily be used to locate persons and because of the growing use of social media. In 2011, several working groups of the national IT summit looked at how to meet these challenges in a process involving federal ministries, business representatives, data protection commissioners and consumer associations. As a first step, a list of tips for users concerning has been compiled, which were published at the IT summit on 6 December 2011.

SLOVENIA / *SLOVENIE*

MAJOR DEVELOPMENTS IN THE DATA PROTECTION FIELD

Report by the Information Commissioner

of the Republic of Slovenia

A. Position and competences of the Information Commissioner

The Information Commissioner of the Republic of Slovenia was established by the Information Commissioner Act[3] (hereinafter: the ICA) that merged two authorities, the previous Commissioner for Access to Public Information and the Inspectorate for Personal Data Protection within the Ministry of Justice. Thus, the Information Commissioner commenced operating on 1 January 2006 as an independent national supervisory authority performing its dual function as the "guardian of the right to know" and as the personal data protection authority. The Head of the Information Commissioner, who has the position of a state official, is appointed by the National Assembly for a 5 year term of office, renewable only once. In addition to adequate legal status, financed directly from the state budget (funding is allocated by the National Assembly on the proposal of the Information Commissioner) and staffed by the officials mandated with full inspection and offence competences, the Slovenian Information Commissioner is qualified to perform its function of data protection authority in entirely independent manner.

Among other competencies determined by the ICA, the Information Commissioner is the inspection and violations authority in the area of data protection in accordance with the Personal Data Protection Act[4] (PDPA), performing also specific supervision functions under special legislation in the areas of patient rights, electronic communications, public media, personal identification and travel documents, and banking.

Of particular importance is the Information Commissioner's competence to lodge an application at the Constitutional Court of the Republic of Slovenia for a constitutional review of law, other regulations and general acts with regard to a procedure being conducted in relation to access to public information or the protection of personal data.

The Information Commissioner is also an independent supervisory authority for the regulation of personal data transfer in accordance with the Schengen Agreement being responsible for the supervision of the national data collection.

[3] Official Gazette of the RS, No. 113/2005.
2 Official Gazette of the RS, No. 94/2007

B. A summary of the activity

Information Commissioner supervision role

In 2011 the Commissioner initiated 682 (599 in 2010) cases regarding **suspected breaches** of the PDPA provisions, 246 (36%) in the public sector and 436 (64%) in the private sector. Compared with previous years (624 cases in 2009, 635 in 2008, 406 in 2007 and 231 in 2006) a dramatic increase in caseload ceased and has been stabilized during last 4 years. In both sectors the most common suspected breaches are of similar nature, involving unauthorised disclosure of personal data by transfer of data to third persons or by unlawful publication of data, unlawful collection of data, inappropriate security of data, abuse of data for the purpose of direct marketing and unlawful video surveillance. Upon the examination of complaints received and due to *ex officio* procedures, 186 **inspection procedures** were initiated against public sector legal entities and 323 against legal entities in the private sector. In 2011 also 136 **offence procedures** were initiated, of which 43 against public sector legal entities, 66 against private sector legal entities, and 27 against individuals. Compared with the previous year the number of inspection procedures (150 in 2010) increased while the number of offence procedures (179 in 2010) decreased.

In addition to the inspection and offence activity the Commissioner performs other tasks as provided by the PDPA. The Commissioner issues **non-binding opinions and clarifications** on specific issues regarding data protection raised by the individuals, data controllers, public bodies and international bodies. In 2011 the Commissioner received 2143 requests (1859 in 2010) that, in addition to a significantly growing trend, are also becoming ever more demanding, which may be attributed to the transparent work and intensive public campaigning of the Commissioner. It is to be added that the Commissioner's staff answer daily to the phone calls related to data protection queries which amount to several thousand every year.

The Commissioner is under PDPA also competent to conduct **prior checks** regarding biometric measures (8 decisions in 2011), transfer of data to third countries (2 decisions in 2011) and connection of public filing systems (8 decisions). The data controllers in such cases need to firstly obtain the Commissioner's permission. Affirmative decisions concerning the implementation of **biometric measures** are granted to those legal entities where it is established that biometric measures are vital to the performance of activities, the safety of employees and property, as well as the protection of classified information or business secrets. Implementation of biometric measures was thus authorised in a case where access to telecommunications room, where servers congaing business secrets and computer equipment of high value were located and needed to be protected. Implementation was also authorised in a case of access to the so called clean spaces in high-tech laboratories where processing and storage of genetic material takes place, in case of laboratories for validation of drugs, in case of objects where devices containing classified information are being destroyed, and in case of an area with an ion accelerator. Prior check is also needed in case of **linking of filing systems** that contain sensitive personal data or if the same connecting code is used for linking. In 2011 authorisation for linking was given to the Supreme Court of the Republic of Slovenia and to the Ministry of Interior in the case of the establishment of e-Land Register, and to the Central Population Register (CPR), general hospital and Ministry of

Interior in the case of e-Birth application, where a link was made between general health records, CPR, and Civil register. The Ministry of Labour, Family and Social affairs was given permission to establish a link between the Central register of the public funds right holders and 15 other registers (e-Social services).

In 2011 the Commissioner received 85 appeals (equally in 2010) concerning the **right to access** one's personal data. However, a repeated increase was noted in the number of cases due to the non-responsiveness of personal data controllers (52% of appeals compared with 38% in 2010 and 51% in 2009), i.e. data controllers who do not respond in any manner to individuals' requests related to accessing their own personal data. Also significant increase has been noted in the appeal procedures concerning access to medical records under the Patients Rights Act (18 appeals in 2011, 4 in 2010 and 8 in 2009).

Under the Constitutional Court Act the Information Commissioner is authorised to initiate the procedure for the **review of the constitutionality or legality** of regulations or general acts issued for the exercise of public authority, provided that a question of constitutionality or legality arises in connection with a procedure it is conducting. In 2011 the Commissioner requested a review of constitutionality of particular Real-Estate Recording Act provisions which because of their vagueness lead the Surveying and Mapping Authority to make certain personal data of the real estate owners registered in building and land cadastres public online. The Commissioner nevertheless holds that the world web should not be understood as appropriate "distribution environment" for the personal data in question, especially in the case of data base of such extent. Furthermore, the constitutionality and legality of the said provisions is questionable for the reason of the uncertainty of the purpose of these personal data processing.

Significant case law

The Commissioner has handled several interesting cases in its inspection procedures and developed rich case law. Below we present some of the cases interesting because of the number of breaches, the weight of the breach or content significance.

Collection of employees' and candidates' data

Privacy at workplace is a problematic area because of vague legal regulation and because of a large scope of offences. In the inspection procedures personnel files are being inspected in order to see what data are being processed by the employers. The employees' personal data may only be processed if stipulated by law therefore employees' consent is not regarded as adequate legal grounds, even though the employers tend to make this argument. Because of unequal power relationship consent in the employment relationship cannot be regarded as freely given. When the Commissioner finds that personal data has been processed without legal grounds (for example data in various questionnaires at the beginning of the employment relationship), the deletion of such data is ordered. According to the law, if the legal basis for processing of personal data ceases to exist, the data must immediately be erased and stop being used. This holds also in the cases of unlawful (often also unmarked) copies of personal documents retained by employers "for the purpose of verification of data accuracy". A distinction also needs to be made between data of the candidates for an open position and employees' data. In the case of candidates, only the data needed for assessment of candidate adequacy may be processed, excluding data such as personal

identification number, tax number or bank account number that may only be processed in the case of employees.

Inadequate security of data in online forum

The Commissioner received a complaint about online matchmaking forum users' names, e-mail addresses and passwords being disclosed online. It has been established that the operator of the website entrusted the design of the website to an Indian contractor, which did not act according to Slovenian legislation. The product did not include measures for traceability of the data processing, and poor programming enabled the perpetrator to gain data on 7000 users of the site. The website operator was also found in breach of the provisions on contractual data processing, because it did not conclude a contract with the data processor. A data transfer to third countries without legal basis was additionally established. The Commissioner ordered the website operator to stop the processing of data and to notify all the users of the forum of the incident. The website operator decided not to establish the forum again, due to the high number of breaches.

Disclosure of personal data in sending e-mails

The Commissioner handled a number of cases where unlawful disclosure of e-mail addresses, regarded as personal data, took place. In all the cases the senders of the message did not put in place appropriate safeguards for data security – all the e-mail addresses were included in the field »To« or »Cc« and were thus disclosed to all the recipients of the e-mail. In one of the cases a notification to unsuccessful candidates for a position was sent by the data controller, who was not aware of the breach, because a dedicated application for handling documentary sources was used for sending the e-mails. The data controller apologised to the recipients and explained what had happened. It instructed its employees on the process of sending e-mails to multiple recipients.

Disclosure of personal data to applicants under the Access to Public Information Act (APIA)

The Commissioner handled a number of cases where public bodies, liable under the APIA, disclosed to the applicants the requested data, whereby also legally protected personal data were disclosed. It has been established that the liable bodies did not take appropriate measures to anonymize certain personal data, such as on the recipient of the document, on education, maiden name or even personal identification number of civil servants. When the requested document contains personal data protected by law, the body has to grant partial access, in the way that personal data in the document are not disclosed.

Publication of images where the individuals may be identified

The Commissioner handled a case where spatial photography containing images with identifiable individuals was published on the website of a professional photographer. The Commissioner stopped the procedure because the photographer removed all the images taken in Slovenia from the website on his own initiative. In the procedure spatial photography was considered in the context of the purpose of publication and identifiability of the individuals in the images. The Commissioner held that images taken and published in the course of reporting on a public event generally do not represent an issue, even if individuals can be identified. In this case the legal interest of the photographer for the publication of the

images overrides the interest of the individual taking part in the public event. However the images of geographical locations, not reporting on an event, but containing images of identifiable individuals are problematic. The Commissioner held that the purpose of depiction of natural and cultural heritage could be achieved also without depiction of identifiable passers-by. The interest of the photographer in the publication in that case doesn't override the interest of the passer-by to decide freely whether he/she wishes to be identifiable in the image. That is why such images have to be rendered anonymous before publication on the internet since the internet brings a new dimension to the publication of images and data protection. The images published on the internet may be accessed by anyone, more and more tools enable facial recognition and the images may be compiled into new filing systems. In its related opinion the Commissioner also pointed to the difference between street photography and spatial photography. The purpose of the latter is depiction of parts of urban areas or architecture, whereas the purpose of street photography is depiction of an individual in public places in special circumstances, situations and interactions.

General state of play of personal data protection in Slovenia

According to the Commissioner a significant increase in cases handled can be attributed to ever higher awareness of Slovenian citizens of their rights on data protection. The Commissioner also found that increasing tendencies on the surveillance of electronic communications are emerging. Such is the case of widening of the scope of competencies of law enforcement regarding the use of data, stored by the operators of the electronic communications (e. g. Data retention). The Government proposed amendments to the Criminal Procedures Act, by which the data on the whole mobile communications base station and not only on one specific phone number could have been acquired by the police. The Commissioner insisted that the approach is highly disproportionate and achieved the removal of the proposed amendment in the Parliament. This is a case that proves one more time that establishment of vast data bases leads to greater appetites for the data and function creep. It also shows lack of impact assessment before establishment of such filing systems, with great impact on privacy. In this context it is necessary to point also to great engagement of the Commissioner in informing the public on ACTA.

The increase of the direct marketing via e-mail was also noted, where the recipients are often not informed about their rights to cancel the use of their data for such purpose. The senders are often unable to explain how the e-mail addresses were gathered. As already mentioned, in this context also a number of cases where e-mail addresses were unduly disclosed, were handled by the Commissioner. In the area of video surveillance we also note an increase, especially in the areas where such surveillance is not lawfully permitted, e. g. in saunas, personnel rooms, lifts and certain public spaces, and for purposes not lawfully permitted such as employee surveillance. Most often the breaches include vague records of access to video surveillance footage and footage use, inadequate information on the implementation of video surveillance, etc. We often note inadequate security of personal data, collected online. In many cases data may be accessed with the use of search engines, where an entered personal name leads to data on e-mail address, user names, and passwords for user accounts on certain portals, or to the data on users that have ordered certain products online.

A number of data controllers are faced with the dilemma whether to use cloud computing services, for all the benefits they offer, such as accessibility, affordability, and flexibility. However cloud computing raises specific risks regarding information security and transfer of data to third countries and doubts regarding its compliance with data protection legislation. The Commissioner has issued and published a number of opinions on this subject and recently also special guidelines on cloud computing have been prepared.

C. Other activities of the Information Commissioner

The Commissioner continued its preventive work, privacy impact assessments in specific planned projects, and actively participated in a number of work groups. It is necessary here to mention the inter-departmental work group where the main focus was establishment of the safer and user friendly e-identities, and inter-departmental work group on the strategy of the information society development in the period between 2011 and 2015.

The Commissioner expanded the scope of its tools for **awareness raising** in the 2011. Along with constant communication with the media, a great number of opinions, guidelines and brochures, published on the website www.ip-rs.si, the Commissioner introduced a new format of special reports that aim to shed light on specific areas that need to be uncovered in terms of data protection practices. The first of the reports covered loyalty cards, an ever more used tool for gathering data on consumers, for segmentation and targeted marketing. The findings were published by a number of media.

Each year the Commissioner also organizes an event on the European Data Protection Day and the World Right to Know Day, on the September 28. The report on the former is dealt with separately. On the occasion of The Safer Internet Day (February 7) the Commissioner joined forces with the Centre for safer internet SAFE.si in public campaigning on this year's theme about connecting generations under the slogan: "Discover the digital world together... safely!"

The Commissioner takes an active role in **preparation of legal acts and other legal documents** by giving an opinion as to the compliance with the provisions on personal data processing, as stipulated by the PDPA. In 2011 the Commissioner advised in preparation of the legislation that governs data processing in health system, underage delinquents, real estate records, road tolling, records of places of residence, electronic commerce and electronic signature, higher education, children with special needs, parliamentary election, tax procedure, criminal procedure, penal code, etc. The Commissioner has also followed closely the development of the new EU Draft Regulation on the protection of personal data and presented its comments and suggestions to the Commission as well as to the Working Party 29.

In terms of **international cooperation** the Information Commissioner as the national data protection authority, cooperates with competent bodies from other EU Member States and the Council of Europe, namely in the Article 29 Working Party, in the Joint supervisory body for Europol (where the Information Commissioner is in the role of the vice president), Schengen and Customs, and in the T-PD under Convention 108. The Commissioner is also active in the International Working Group on Data Protection in Telecommunications and in the Working Party on Police and Justice.

The rich international activity is complemented with attendance at international meetings, such as the International Conference of Data Protection and Privacy Commissioners and International Conference of the Information Commissioners. The latter has given a mandate in Ottawa to the Slovenian Information Commissioner to establish a website of all the Information Commissioners, that was presented to the public in November. Experts of the Information Commissioner have actively participated in a number of international seminars and workshops.

The Information Commissioner participates as a Junior Partner in a twinning project »Implementation of Personal Data Protection Strategy« in Monte Negro. At its seat it hosted representatives from similar authorities from Croatia, Serbia, Kosovo, Monte Negro and Macedonia.

The activities of the Commissioner are widely publicized. Therefore it is not surprising that in national public opinion research (Politbarometer) the Information Commissioner ranks first among the state bodies and public institutions that citizens trust the most.

Nataša Pirc Musar,

Information Commissioner

of the Republic of Slovenia

SWITZERLAND / SUISSE

Développements majeurs intervenus en Suisse depuis la 27ème réunion du T-PD

Évaluation de la loi sur la protection des données

Une évaluation de la loi fédérale sur la protection des données a été effectuée sur mandat de l'Office fédéral de la justice. L'évaluation montre que d'une manière générale la LPD permet en soi d'atteindre les objectifs visés. Elle débouche cependant sur un constat selon lequel les menaces qui pèsent sur le respect des droits et des libertés fondamentales lors du traitement de données personnelles se sont renforcées ces dernières années. Les individus ont toujours plus de peine à conserver la maîtrise sur les données qui les concernent. L'évolution technologique et le volume de données qu'elle engendre sont des défis considérables non seulement pour les individus, mais aussi pour les responsables de traitement et les autorités de protection des données. Ainsi les évaluateurs reconnaissent que si le préposé fédéral remplit son mandat légal avec un haut degré d'efficacité, il rencontre néanmoins « des difficultés croissantes à exercer son mandat de surveillance étant donné l'accroissement constant de la fréquence, de l'opacité et de l'internationalisation des traitements. ». Ils relèvent un déficit au niveau de l'exercice des droits des personnes concernées. Ce déficit découle notamment du fait du coût et de la longueur des procédures. Il provient également du fait de l'importance et l'ampleur des données collectées quotidiennement et du fait que trop souvent les personnes ne prennent pas suffisamment conscience que des données sont collectées et traitées à leur égard. Le Conseil fédéral dans un rapport qu'il a adressé au Parlement convient que la loi sur la protection des données doit être adaptée « aux rapides développements technologiques et sociétaux intervenus depuis son entrée en vigueur » et « prendre en compte les nouvelles menaces. » Il a donné mandat au Département fédéral de justice et police de faire des propositions d'ici 2014.

Ce travail de mise à jour et de révision de notre droit de la protection des données devra tenir compte des travaux en cours au sein de l'Union européenne en vue d'un nouveau cadre juridique de protection des données et au Conseil de l'Europe avec la révision de la Convention 108. Le Conseil fédéral souhaite également examiner la répartition des compétences entre la Confédération et les cantons en matière de législation et de mise en oeuvre, ainsi que l'introduction de mesures d'autoréglementation et un renforcement éventuel de l'indépendance du Préposé fédéral à la protection des données et à la transparence.

Modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

Dans le cadre de la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, le régime du droit d'accès des personnes concernées a été modifié. Dès le 1er juillet 2012, les personnes concernées bénéficieront d'un droit d'accès direct et s'adresseront directement au service de renseignement de la Confédération pour faire valoir leur droit. L'accès pourra cependant être différé dans trois cas :

- Les données traitées concernant le requérant sont liées à des intérêts prépondérants qui exigent le maintien du secret dans le cadre de la détention précoce et de la lutte contre les dangers en matière de terrorisme, de service de renseignement prohibé, d'extrémisme violent, des actes préparatoires relatifs au commerce illicite d'armes et de substances radioactives et du transfert illégal de technologie ainsi que dans le cadre d'une poursuite pénale ou d'une autre procédure d'instruction.

- Les intérêts prépondérants d'un tiers l'exigent

- Aucune donnée concernant le requérant n'est traitée.

En cas de refus ou de report de la demande de renseignement, le requérant en est informé et a la possibilité de demander au Préposé fédéral à la protection des données et à la transparence de vérifier le traitement. Le préposé peut en cas d'erreur adresser une recommandation au service concerné. Il informe le requérant qu'aucune donnée le concernant n'est traitée illégalement ou qu'en cas d'erreur relative au traitement ou au report de la réponse, une recommandation a été adressée au service concernée. Suite au contrôle du préposé, le requérant peut s'adresser au Tribunal administratif fédéral. En cas d'erreur, le Tribunal adresse au service concerné une décision lui ordonnant d'y remédier. Le service concerné communique au requérant les renseignements qu'il a demandés dès que les intérêts liés au maintien du secret ne peuvent plus être invoqués, mais au plus tard après l'expiration du délai de conservation. Le requérant qui n'est pas enregistré en est informé au plus tard trois ans après réception de sa demande. Le préposé peut exceptionnellement recommander de fournir immédiatement le renseignement demandé lorsque cela ne menace pas la sûreté intérieure ou extérieure.

Outil de sensibilisation à la protection des données et à la transparence (Thinkdata.ch)

A l'occasion de la 6e journée de la protection des données, le 28 janvier 2012, un outil de sensibilisation à la protection des données et à la transparence (Thinkdata.ch) a été présenté et mis en ligne (version en français actuellement). Cet outil interactif s'adresse aux administrations et aux entreprises, ainsi qu'aux utilisateurs et aux personnes concernées par les traitements de ces organisations, en fonction de leur métier ou de leur rôle dans l'organisation (cadres, responsables des ressources humaines, responsables IT, employés, …). L'outil présente sous l'angle des métiers mais également des types de données différents scénarios inspirés d'histoires réelles. Ces scénarios relatent un problème lié à la protection des données ou à la transparence dans le but de sensibiliser l'utilisateur de l'outil. Des conseils sont associés aux scénarios pour permettre aux utilisateurs de se positionner et d'améliorer le traitement des données au sein de leurs organisations

Suite aux réactions positives reçues depuis la mise en ligne de ce service, une deuxième version est en préparation. Elle devrait en particulier être multilingue (notamment allemand et anglais) et si possible déborder le cadre purement helvétique.

Le service est accessible sous www.thinkdata.ch

Rapport d'activité

Le Préposé fédéral à la protection des données et à la transparence présentera son 19e rapport d'activités lors de sa conférence de presse annuelle, le 25 juin prochain. Le rapport pourra être consulté sur www.edoeb.admin.ch