Personal Data Protection

Coordinator **LDH** Ligue des droits de l'Homme

Partners **AEDH – EDRI – IURE - PANGEA**

CZECH REPUBLIC NATIONAL REPORT - IURE

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH, EDRi, AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

December 2009

SOMMAIRE

Introduction and methodology

The focus of this report has been shaped by the two brainstorming events and respective outputs:

1. Debates and minutes produced during the "kick-off" meeting in Paris on 13th February 2009, where there were identified four main areas of the research:

- **Mobility and transportation**
- **Biological identity**
- **Interpersonal communications**
- **Social networks as new gate keepers of communications**

The structure of the report and a common matrix grid has been also agreed on.

2. Debates and meetings of the Iuridicum Remedium team members, during which a most suitable approach and also concrete cases to be included were identified. In these discussions, following selection criteria specific cases were adopted:

- The case should represent **general trends**
- The case should be related to **latest development of new technology or policy**
- The case should be relevant to **youngsters** (their data being exceedingly at stake).

The research has been extensively (but not exclusively) based on the following main resources:

a) Results of the previous expertise, findings and campaigns of the Iuridicum Remedium team
b) Nominations submitted by the general public to the Big Brother Awards contest organised by Iuridicum Remedium – include more than 70 state and non-state actors affecting privacy[1]
c) Annual report 2008 of the Czech DPA
d) Consultations with external experts, namely Karel Neuwirt (former chief of Czech DPA), Jiří Peterka (Faculty of Mathematics and Physics of Charles University, journalist and IT expert at lupa.cz), Jiří Šimůnek (Ropid, transportation expert), Tomáš Rosa (eBanka, cryptologist).
e) Responses to questionnaires prepared and sent out by Iuridicum Remedium
f) Media monitoring and research
g) Research on the current legislation

On the basis of discussions within the project team (LDH, EDRi, Pangea and Iure), discussions within the Iuridicum Remedium team (Filip Pospíšil, Marek Tichý, Helena Svatošová), consultations with experts and preliminary research, the structure and questions of the questionnaire were defined and relevant actors identified. During March, April and May, personalized questionnaires were submitted to the following **target institutions**:

- Ministry of Interior
- Presidium of Police
- Institute of health information and statistics of the Czech republic
- State Institute for Drug Control
- Institute for information on education
- VZP ČR (largest Czech health insurance company)
- ZPMVCR (Health insurance company of the ministry of interior)
- DNAtest.cz (company offering genetic testing)

1 Up-to-date list of nominations can be found at http://www.slidilove.cz/nominace/aktualni

- GTS ALIVE s.r.o. (largest company offering student cards)
- Secondary technical school in Prague 10 (one of the biggest school with elaborated card system)
- Seznam.cz (company operating social network services Lide.cz and Spoluzaci.cz)
- Libimseti.cz (company operating social network service)
- Czech airlines
- Czech railways and HAGUESS, a.s. (operator of the Prague rfid based opencard).

From all the approached state institutions and companies none responded to the questionnaire in full. Ministry of the Interior has responded on the 20th April 2009 asking for 11295 Kč (approx. 420 Eur) as a fee for research and administrative costs related to the response to the request. After the payment, the ministry sent on 29th April 2009 a letter containing a list[2] of 21 databases operated by the ministry. However, some information regarding the specification of the data stored, data subjects, data retention periods, access restrictions and purpose of storage were in many cases either totally missing or defined just with a broad reference to an individual Act etc. Iuridicum Remedium has filled an an appeal to the Minister of Interior on 11th May 2009. In his response to the appeal Minister of Interior Martin Pecina on 3th of June 2009 acknowledged that some information in the response were missing and requested ministry to prepare new response withing 15 days after the delivery of his decision. Minister however refused to return the fee.

Police presidium responded on 5th of June with a letter containing a list[3] of 35 databases operated by the Czech Police. There were however missing information regarding some of the databases related to the category of the data stored, whose data are stored, period of data retention, regulation of the access to the files, purpose of storage was in many cases defined just with broad reference to individual Act etc.

Iuridicum Remedium is about to initiate a court proceeding with two above mentioned institutions according to the Act No. 106/1999 Coll. on Free Access to Information which covers the "state agencies, territorial self-administration authorities and public institutions managing public funds" as well as any body authorized by the law to reach legal decisions relating to the public sector, to the extend of such authorization.

Institute for information on education and Institute of health information and statistics of the Czech republic has responded partially. The rest of the state institutions and private companies have not filled the questionnaire. **It is important to emphasize that the Freedom of Information Act doesn't apply to private companies. None of the institutions and companies has also provided information on how they process personal data of clients, patients, users etc. publicly available (for instance at their web pages) neither in Contracts, Rules of use etc., even though the Act 101 of April 4, 2000 on the Protection of Personal Data stipulates:**

"(4) When giving his consent the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. "

In case of the state institutions where processing of a data is regulated by a special law and consent of the data subject is not required, information policy regarding data processing is very poor. **Insufficient information policy of the controllers and processors of the data towards data subjects is one of the first and major findings of this research.**

Privacy related legislation

Definitions, core concept and scope of data protection in the Czech republic are defined by Personal

2 *Table enclosed*
3 *Table enclosed*

Data Protection Act Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts.[4] This Act, in accordance with the law of the European Communities, international agreements binding the Czech Republic provides for exercising of everyone's right to the protection from unauthorized interference with privacy, regulates the rights and obligations in processing of personal data and specifies the conditions under which personal data may be transferred to other countries. The Act implements the requirements of the EU Data Protection Directive, granting exceptions from several key provisions to the police and intelligence services in matters of public and national security in accordance with the directive. Data controllers were required to register their systems and fully comply with the Act by June 1, 2001. A May 2001 amendment exempted political parties, churches, sports clubs, and other civic organizations engaged in standard and legitimate activities from some of the Act's requirements, such as registering their data processing activity or obtaining consent of individuals before collecting personal information.

A June 2004 amendment to the Banking Act completed harmonization with EU Data Protection Directive (1995/46/EC).5 The amendment refines certain terms, as well as, introduces new terms in accordance with the EU directive. The amendment includes terms regulating the granting of consent for personal data processing, the relationship between data controllers and data subjects, the notification duty of controllers, and indemnification of data subjects for breaches of duty committed by data controllers or data processors.6

Another type of international obligations that effect privacy are treaties and agreements related to in the area of Law enforcement and intelligence cooperation (cooperation within SIS, VIS, CIS, EURODAC systems, PNR transfers to the US, etc.)

On the constitutional level the 1993 Charter of Fundamental Rights and Freedoms provides for extensive privacy rights. Article 7(1) states, "The inviolability of the person and of privacy is guaranteed. They may be limited only in cases provided for by law." Article 10 states, "(1) Everyone has the right to demand that his human dignity, personal honor, and good reputation be respected, and that his name be protected. (2) Everyone has the right to be protected from any unauthorized intrusion into her private and family life. (3) Everyone has the right to be protected from the unauthorized gathering, publication revelation, or other misuse of his personal data." Article 13 states, "Nobody may violate confidentiality of letters or other papers or records, whether privately kept or sent by post or by some other means, except in cases and in the manner specified by law. The confidentiality of communications sent by telephone, telegraph or other such devices are guaranteed in the same way."7

Data protection authority

The Office for personal data protection was established in 2000 as an independent supervisory body

of the State. It consists of 7 inspectors appointed for a period of 10 years by President of the Czech Republic on the basis of a proposal of the Senate of the Parliament of the Czech Republic. The Office has its president and approx. 92 employees (December 2008). The Office runs the register of data controllers and processors, does inspections with the aim to prevent illegal processing of personal data. Office on some occasions comments on proposed legislation however it was not yet been given its own legislative initiative and "*has often found itself in a difficult position where, on the one hand, the public rightly expected expeditious and effective intervention by the Office, particularly with respect to State powers and public administration performed by governmental bodies, and, on the other hand, legal regulations provided and still provide, in spite of the generally applicable principles of privacy protection, for further and more extensive authorizations or exemptions related to personal data processing beyond the scope of the Personal Data Protection Act, both in private law and in public law. Indeed, when the Office's attempts to enforce its opinions and control findings with respect to the special conditions of*

---

4 Consolidated version of the Personal Data Protection Act at <http://www.uoou.cz/uoou.aspx?menu=4&submenu=5>

5 Act No. 439/2004 Coll. (2004), http://portal.gov.cz/wps/portal/_s.155/701?number1=439%2F2004&number2=&name=&text=

6 Office for Personal Data Protection Annual Report 2004, at 31, available at <http://www.uoou.cz/rep_2004.pdf>.

7 Charter of Fundamental Rights and Freedoms, 1993, available at <http://test.concourt.cz/angl_verze/rights.html>.

personal data processing in a certain area are confronted with its actual supervisory competence, the Office must often surrender its categorical viewpoint given the existence of a special regulation that prevails over the Personal Data Protection Act. However, the basic legal conditions are thereby unevenly applied to processing and protection of data and certain groups of controllers are favored solely because their activities are defined by a special regulation, even though no such regulation should in fact exist in the framework of the general principles of protection of privacy and protection of personal data."[8]

Privacy awareness

From the Office for Personal Data Protection 2007 Annual Report[9],

"We can witness a shift in the pendulum towards collective security, as well as comfort, to the detriment of the right to privacy. This is all happening with the uninformed consent of a majority of the population. It is clear that even a number of responsible officials do not realize that invasive intervention in the privacy of citizens could ultimately be a means of breaching the safety of us all."

On the positive side, due to the public work of the Office for Personal Data Protection as well as the efforts of expert NGOs like the privacy watchdog Iuridicum Remedium[10], the general awareness of the double edged nature of various national and private security, e-government, e-health and commercial measures among the general society seems to be on a slow but steady rise. In 2008, more than thousand people have joined the local Freedom Not Fear march[11], a part of the multinational protest movement against the disproportionate intrusions into citizen's privacy. NGO Iuridicum Remedium organized in autumn 2009 fifth annual Big Brother Awards Ceremony pointing on worst privacy intruders. DPA runs several educational activities and awareness programs for teachers and small children.

Mr Nemec in his foreword continues:

"However, I am also glad that we have been and continue to be able to discuss these aspects with the public and that our citizens are becoming increasingly aware of the risks related to a careless attitude towards their property – personal data – which is reflected in an increasing number of questions, complaints and registrations."

The trend of increase in numbers of questions, complaints and registrations, which in fact becomes to overstretch capacities of the Office for Personal Data Protection can be demonstrated by following data. In the 2008 alone the Office reported 1 813 questions from the public, 697 complains, 3 327 submissions for registration.[12] Year before it was 1274 questions, 574 complains, 30 806 submissions for registration.[13]

---

[8] *Czech DPA Annual report 2006, p. 10*

9 *UOOU Annual Report 2007, http://www.uoou.cz/files/rep_2007.pdf*

10 *Iuridicum Remedium (www.iure.org); Human Rights and Technologies (www.bigbrotherawards.cz)*

11 *FNF 2008 EDRigram coverage: http://www.edri.org/edri-gram/number6.20/prague-freedom-not-fear*

[12] *UOOU Annual report 2008, http://www.uoou.cz/files/vz_2008.pdf*

[13] *UOOU Annual report 2007, p.6*

Summary and findings

Mobility and transportation

Two of the selected examples (IN-card of the Czech railways and Pragues´Opencard) shows the extend and risks of a newly introduced RFID chip technology in cards, which is used as a season discount cards in public transportation. Both projects were rolled out without a proper assessment of the privacy risks and these risks have not been properly analyzed even two years after the start of the project. Projects also sneakingly broadens its scale (introduction of other services and other groups of users). They do not provide user with the possibility of choice for anonymous service for an adequate costs. Users are not properly informed of the extend to which their personal data are being processed neither about their rights regarding the retained data. As DPA Annual report 2008 states on the results of its inspections of RFID related projects: "It can also be inferred from the course of the controls that, neither in decision-making on introduction of the new technology nor in the preparation of the relevant projects are the duties following from the Personal Data Protection Act taken into account." In this respect arises a question whether adoption of a new legislation specifically dealing with RFID chips could improve the situation.

Third example of a technology in this chapter - PNR data transfers - shows the persisting practice of personal data transfers contravening European legislation and trends towards enlarging of controversial practice worldwide including attempts to include EU PNR scheme.

Biological identity

There are two cases represented in this study. One state institution (National DNA database) and one private company (Genomac) dealing with a new technology of DNA analysis and related databases of profiles and DNA samples. In both cases there were serious misconducts confirmed recently by the inspection of the Czech DPA. Both cases also demonstrate the need for a new legislation regulating specifically the DNA databases, and also the necessity of broader public awareness campaign on privacy risks related to compromising of sensitive information contained in DNA profiles.

Another example in this chapter show an increasing trend in creating databases of state health policy institutions containing sensitive information on health status of the patients. Fourteen eHealth registers were created in recent years without a clarification of their purpose and respect to free consent of the patient with the procession of data. The terms of data retention of those registers also seems to be defined rather randomly. A new register which is have been built since early 2009 till the end of summer 2009 – The Central repository of electronic prescriptions – even lacked legislative basis and there were indications that due to the outsourcing of the sensitive data processing, those may have ended up in the hands of private health insurance companies.

Interpersonal communications

The example of the greatest scale of data gathering and retention is that of the providers of telecommunication and electronic communication. The necessity of an assessment of the legislation and practice by the Constitutional court, as well as broader public discussion on a practice of retention of data on electronic communication is demonstrated here.

Social networks as new gate keepers of communications

For this chapter the team has selected four cases of most popular social networking services in the Czech republic. Despite series of awareness campaigns by service providers, DPA, state institutions and NGOs targeted on young users of the services and protection of the privacy on the Internet, companies providing service of social networks have not adopted transparent information policy on the way they process or share the data of their users. Some of the security arrangements introduced by the providers

of the services were found insufficient. Despite the fact there has been recently some public discussions on the risks related to the misuse of posted data on the internet (for instance for profiling candidates for employment by companies), many of the users are still ignoring possible risks.

Databases of the data of the youth

Apart from the four defined areas of research the Iuridicum Remedium team has also decided to add two more cases to the report. This decision has been supported by previously declared ambition of the report to reflect on the practice of data protection and data protection risks with special emphasis on protection of the data of the youth. In the last decade, state authorities responsible for education policy started to create centralized databases of personal data of general population of students and pupils. However, the whole concept of these registers is unclear, sometimes lacking a proper legislation. Free consent of the students with the procession of the data is not respected, assessment of the privacy risks was not properly completed. Information on measures on right to access and edit the data, auditing of access to the data are not publicly available.

Recommendations

Mobility and transportation

Rule of obligatory introducing of anonymous cards instead of non-anonymous cards when possible should be clearly established by new legislation or “softer” transport company code of conducts. Regular privacy assessment procedure (Privacy Impact Assesment) for any RFID related project with possible bigger impact on the citizens rights should be established. This procedure might be done by independent auditing organisation, published and submitted to the DPA.

Biological identity

Any newly established or already existing databases of biological data needs to greatest possible extend respect the principles of free and informed consent of the patient with the procession of the data, clearly define data retention periods and clearly define purpose of procession of the data. Legislation change especially in the area of DNA processing would be probably necessary. Any newly prepared legislation (on e-health and similiar databases) must adhere to the principles of data protection. Campaign raising awareness of risks related with procession of sensitive information for health specialists as well as for broader public would be useful in this context.

Interpersonal communication

Constitutionality of the provisions and practice of the data retention should be assessed by the Czech Constitutional Court.

Awareness campaign on fundamental right to confidential communications guaranteed to the individuals by Article 8 of the European Convention on Human Rights, awareness campaign on actual practice and extend of a traffic and location data stored by ISP and telecommunication providers and transfered to the Police should be organized.

Social networks

Special focus need to be given to the practice of retaining of a data even from cancelled profiles and rules of transfer and procession of a data by a third parties (government bodies, other service providers, marketing and advertising companies). Companies providing service of social networks has also to adopt transparent information policy on the way they process or share data of the users.

Awareness campaign needs to be organized on rights of the users of the social networks and implementation of better privacy protection practices by individual companies and better informing on the way how they processes personal data.

Databases of the data of the youth

Reasons for collecting of the data and the same concept of centralised students and youth registers should be clarified. Clear legal bases of the registers must in greatest possible extend respect the principles of free consent of the students/parents with the procession of the data. System of identification of the students by their birth number must be replaced with source identifier. Clear and strict measures on right to access and edit the data, auditing of access to the data should be imposed.

Awareness campaign on extend of data currently processed and importance of free consent with data protection need to be organized.

1-MOBILITY AND TRANSPORTATION

11 - PRAGUE OPENCARD

Technology used/tool (For each teams, a card pro tool)	**RFID CARD/ smart – card**
Country/ use area	Czech republic/ Prague
Frame of use	Used as season ticket for public transport, as library card for city library and prepaid car for parking in the city centre
Population concerned: target and age	General population, users of season discount card and cards for pensioners, students, children
% of users/of young users	Unknown
Trends (measured / supposed)	Number of users was 8 thousands in 2008 and reached to 330 thousands in mid march 2009[14] after RFID card was made obligatory for anyone seeking annual discount card for 2009.
Known or potentials dangers /Risks	In 2007 it was revealed by cryptologist Tomáš Rosa that data on first name, family name of the users as well as their date of birth was possible to read with common RFID reader from some distance without knowledge of the user from chip Mifare Classic due to lack of proper encryption of the data. Later versions of the card contain chips MIFARE DESFire with more proper encryption.[15] Inspectors were equipped with an RFID readers in 2008. In the late 2008 city authorities announced a plan to introduce turnstiles in the city transportation that would facilitate reading of the data from the smart-card.[16] Information on unique ID of the RFID chips can be gathered from inspectors and turnstiles when related to already created database of card holders may establish a new database enabling tracking movement of the users.
Others	Currently information on the card include : first name, surname and a photograph printed on the card. Date of birth is recorded in encrypted form to the contactless chip, as well as the unique identification number of RFID on each card and other certified

[14] press release of the project opencard http://opencard.praha.eu/jnp/cz/aktuality/pro_media/podminky_pro_nahravani_kuponu_pid_na.html
[15] press release of NGO Iuridicum Remedium of 29.7.2007 http://zpravodajstvi.ecn.cz/index.stm?x=2020676

16 Chris Johnstone, Prague transport company seeks to bring back metro turnstiles, 18.3.2009 in http://www.radio.cz/en/article/114326

	data of the providers of the services.
Generated data bases	
Associated data base/ creation (a line pro database)	First name, surname, date of birth, photograph of the holder face, academic title (voluntary), gender (voluntary), ID number of request, unique ID of the card, authentification codes, home adress of holder, email adress (voluntary), telephone number (voluntary), ID card or passport number, signature, date of submitting request for card, date of issuing the card, data related to the usage of a card are stored in the main operator's database (City of Prague)[17], service providers (library, city transport) gather information on specific transactions done by the users
What justifies the inscription in the file /Risks?	Operator argues that **c**ontact data serves for day-to-day communication with card holders, date of birth is needed when applying for the age-related discount and personal data is generaly needed so inspectors can recognise authorised user of the card. Data protection office argues however : «*To find out whether holder of the card is or is not authorised user the operator doesnot need to keep a database of all* **persons whom he issued card to**»[18]
Purposes /contents, main data included / Risks?	See above
File masters? Risks?	City of Prague, Pražské centrum kartových služeb (Pragues center of card services, PCKS), Dopravní podnik hlavního města Prahy (Prague public transport company, DPP), Městská knihovna v Praze (City library, MKP) - these are «controllers» responsible for processing the collected data according to the law, they furhtemore empower private «processors» to process and store collected data: HAGUESS, a.s., (ID of organisation 250 85 166), Asseco Czech Republic, a.s.. (27074358), Monet+, a.s., (262 17 783), STÁTNÍ TISKÁRNA CENIN, státní podnik, (000 01 279), Městská knihovna v Praze (00064467), Dopravní podnik hl. m. Prahy, akciová společnost (000 05 886), Cross Point, s.r.o. (278 73 200), Pasante s.r.o., (267 26 840), V.P., a.s.,(282 10 999)[19]
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Information on security measures applied on access to the data processed by individual „controllers" and „processors" are not available. There are a subject of prolonged inspection of Data Protection Office. Results of that inspection were so far not announced. Beside processing of the data collected from individual service applications on the card, the main „controller" City of Pratur

[17] *conditions of the contract – opencard http://opencard.praha.eu/jnp/cz/podminky/zpracovani_osobnich_udaju.html*
[18] *Czech Data protection authority Annual Report 2008*
[19] *conditions of the contract – opencard http://opencard.praha.eu/jnp/cz/podminky/zpracovani_osobnich_udaju.html*

	shares with Dopravní podnik hl. m. Prahy, akciová společnost (000 05 886) unique ID of the card, date of birth of the holder, information on blocation of the card. With Městská knihovna v Praze (00064467) City of Prague shares unique ID of the card, information on blocation of the card.[20]
Data retention delays/ risks Right to be forgotten	Data retention period varies according to a type of a data from 30 days after the contract was canceled by a user or the service was finished to 5 years and 30 days for a data „necessary for protection of the rights and interests of the collectors, processors or receivers of the data“. Individual operators of the applications on the card may set their own time limits for retention of the data.
Rights to know or to modify data?	Any subject of a data (holder of a card) can ask „processor“ or „controller“ on information if and what of his/her data he processes. „Controller“ on the other hand can ask the holder to pay necessary cost related to submitting of this information. Holder of a card can ask „procesor“ or „controller“ to modify the data and may complain to Data protection autority if his/her request is refused.
Covert purposes/ Risks/uncontrolled future evolution	Hardware of the system and its applications enable covert collection of a data on customers/holders behaviour, habits, usage of services (travelling habits, reading preferencies, etc.). Establishing of universal smart-card in its non-anonymous version forces holders to use services formerly offered on anonymous basis or without massive electronic procession of a data. Free consent of the user with processing his/her data becomes illusionary as the services on anonymous basis are offered for much higher price and/or are not available any more without using of non-anonymous card. The reasoning for discriminatory pricing of anonymous card given by the operator stated, that anonymous card can be shared by more people. This argument however doesnot stand the criticism that the purpose of preventing use of the card can serve simple photograph of the holder printed on the card and no data need to be than stored in the database. Another reasoning in against creating of database of the data of the holder has presented Czech DPA in its 2008 Annual report : « It has also been shown that transport documents – cards with an RFID chip – can be issued in a manner where the personal data including the name, surname and photograph are merely printed on the card and not stored in a database. A reason frequently put forth by the transport companies, i.e. that a list of persons to whom a card has been issued serves for these persons themselves in case of theft or loss of their card, so that the card can be readily and quickly blocked, thus preventing its misuse by an unauthorized

[20] *conditions of the contract – opencard http://opencard.praha.eu/jnp/cz/podminky/zpracovani_osobnich_udaju.html*

	person, must be rejected, as the law prefers means that do not interfere with privacy and do not threat personal data. Indeed, it is very easy to provide each card holder, upon issuing the card, with confirmation of delivery (payment) of the card, which may contain information on the type and number of the card, as well as the name and surname, if appropriate, which can be used to demonstrate the authorization to hold the card and the paid application. The card can be immediately blocked according to the number of the card set out on the document. However, in practice, the issuer of the card, as a personal data controller, himself makes a decision for the passenger, does not allow the passenger to manifest his free will and, moreover, patronises the citizen."
Others (interconnections…)	Complex relations between different data "controllers" and "processors" and complex technical solutions and processes make virtually impossible for user to realise the way it is being dealt with his/her data and asses related risks.
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	No specific legislation on RFID use Personal Data Protection Act, Act 101 of April 4, 2000 Chapter II Rights and obligations in processing of personal data Article 5 (1) The controller shall be obliged to: (a) specify the purpose for which personal data are to be processed; (b) specify the means and manner of personal data processing; (c) process only accurate personal data, which he obtained in accordance with this Act. If necessary, the controller is obliged to update the data. If the controller finds that the data being processed thereby are not accurate with respect to the specified purpose, he takes adequate measures without undue delays, in particular he blocks the processing and corrects or supplements the personal data, or otherwise he must liquidate the personal data. Inaccurate personal data may be processed only within the limits of the provisions of Article 3(6) of this Act. Inaccurate personal data must be branded. The controller is obliged to provide all the recipients with the information about blocking, correction, supplementing or liquidation of personal data without undue delay; (d) collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfilment of the specified purpose; (e) preserve personal data only for a period of time that is necessary for the purpose of their processing. After expiry of this period, personal data may be preserved only for purposes of the

	state statistical service, and for scientific and archival purposes. When using personal data for these purposes, it is necessary to respect the right to protection of private and personal life of the data subject from unauthorised interference and to make personal data anonymous as soon as possible; (f) process personal data only in accordance with the purpose for which the data were collected. Personal data may be processed for some other purpose only within the limits of the provisions of Article 3(6) or if the data subject granted his consent herewith in advance; (g) collect personal data only in an open manner. Collecting data under the pretext of some other purpose or activity shall be prohibited; (h) ensure that personal data that were obtained for different purposes are not grouped. (2) The controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data: (a) if he is carrying out processing which is essential to comply with legal obligation of the controller; (b) if the processing is essential for fulfilment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the data subject; (c) if it is essential for the protection of vitally important interests of the data subject. In this case, the consent of data subject must be obtained without undue delay. If the consent is not granted, the controller must terminate the processing and liquidate the data; (d) in relation to personal data that were lawfully published in accordance with special legislation. However, this shall not prejudice the right to the protection of private and personal life of the data subject, or (e) if it is essential for the protection of rights and legitimate interests of the controller, recipient or other person concerned. However, such personal data processing may not be in contradiction with the right of the data subject to protection of his private and personal life. (f) if he provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity, their functional or working position, or (g) if the processing relates exclusively to archival purposes pursuant to a special Act. (3) If the controller processes personal data on the basis of a special Act, he shall be obliged to respect the right to protection of private and personal life of the data subject. (4) When giving his consent the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. The controller must be able to prove the consent of data subject to personal data processing during

	the whole period of processing. (5) If the controller or the processor carries out personal data processing for the purpose of offering business opportunities or services to the data subject, the data subject's name, surname and address may be used for this purpose provided that the data were acquired from a public list or in relation to his activity of controller or processor. The controller or processor, however, may not further process the data specified above if the data subject has expressed his disagreement therewith. The disagreement with processing must be expressed in writing. No additional personal data may be attached to the data specified above without the consent of data subject. (6) The controller who process personal data pursuant to paragraph 5 may transfer these data to some other controller only if the following conditions are met: (a) the data on the data subject were acquired in relation to activities of the controller or the data in question consist in published personal data; (b) the data shall be used exclusively for the purpose of offering business opportunities and services; (c) the data subject has been notified in advance of this procedure of the controller and the data subject has not expressed disagreement with this procedure. (7) Other controller to whom data pursuant to paragraph 6 have been transferred may not transfer these data to any other person. (8) Disagreement with processing pursuant to paragraph 6(c) must be expressed by the data subject in writing. The controller shall be obliged to notify each controller to whom he has transferred the name, surname and address of the data subject of the fact that the data subject has expressed disagreement with the processing. (9) To eliminate the possibility that the name, surname and address of the data subject are repeatedly used for offering business opportunities and services, the controller shall be entitled to further process the subject's name, surname and address in spite of the fact that the data subject expressed his/her disagreement therewith in accordance with paragraph 5. Article 6 Where authorization does not follow from a legal regulation, the controller must conclude with the processor an agreement on personal data processing. The agreement must be made in writing. In particular, the agreement shall explicitly stipulate the scope, purpose and period of time for which it is concluded and must contain guarantees by the processor related to technical and organisational securing of the protection of personal data. Article 7 The obligations specified in Article 5 shall apply to the processor mutatis mutandis. Article 8 If the processor finds out that the controller breaches the obligations provided by this Act, the processor shall be obliged to

	notify the controller of this fact without delay and to terminate personal data processing. If he fails to do so, the processor and the data controller shall be liable jointly and severally for any damage incurred by the data subject. This shall in no way prejudice his responsibility pursuant to this Act.
Risks for freedoms despite the law	Complex technical and organisational solution makes very difficult to asses privacy related risks even to experts (DPA) not speaking about common user. Formerly anonymous or semi-anonymous usage of public services is becoming less possible allowing the service providers to track behaviour to track behaviour of the users. Availability of the services is becoming more linked to the assigned electronic (not physical) identity of the user. Loss or damage of an electronic card proving electronic identity might limit access to a citizen to a public services. Leakage of a collected data might further compromise privacy of the user to a third (commercial) parties.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Practice might contravene: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001. Article 5 – Quality of data Personal data undergoing automatic processing shall be: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. Article 7 – Data security Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. Article 8 – Additional safeguards for the data subject

	Any person shall be enabled: a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	Create significant part of the users, number not revealed
Awareness of issues or of risks	Partial, no specific public debate on the risks and function of unique identifiers
Indifference or reaction	1000 signatures under the petition for introduction of anonymous smard-card (organized by Iuridicum Remedium)
Awareness campaigns/ results	Campaign by Iuridicum Remedium led to introduction of better encryption of a data contained in the RFID chip of the card, start of DPA inspection, series of articles on privacy related issues to the project of smart card, number of interpellation by city deputies of city government and launch of a petition for introduction of anonymous card
Good practises	Introduction of better encryption of data on a card
Campaign to be led. On which themes?	Further campaign on introduction of an anonymous card issued at non-discriminatory (pricing) conditions
Others	
Conclusions	Project of the open card (smart-card) was introduced without proper assessment of the privacy risks and these risks are not properly analysed even two years after the start of the project.

	Project meanwhile broadens its scale and city government introduces new conditions on the use of the public services, which make free consent of the users with processing of their data illusionary
Recommendations	Establishing a rule of obligatory introducing of anonymous cards instead of non-anonymous cards when possible Establishing a regular privacy assessment procedure (Privacy Impact Assesment) for any project with possible bigger impact on the citizens rights. This might be done by independent auditing organisation, published and submitted to the DPA. Impulse for greater respect to the privacy by operators of the RFID systems might create establishing a new legislation specifically focused on RFID.

12 - PNR

Technology used/tool (For each teams, a card pro tool)	Database
Country/ use area	World/US/EU/ Czech republic/
Frame of use	Booking of air tickets, itinerary and personal information of a passenger, or a group of passengers traveling together by plane used for profiling of passsengers allegedly for crime prevention.
Population concerned: target and age	General population, clients of airline companies
% of users/of young users	Unknown
Trends (measured / supposed)	(according to wikipedia[21]): Access and transfer of PNRs fall under the purview of European Data Protection Law. Under the Organisation for Economic Cooperation and Development (OECD) 1980 Privacy Guidelines, and the 1995 European Union Directive on data protection, PNRs may only be transferred to countries with comparable data protection laws. Also, law enforcement authorities are permitted to access the passenger data only on a case-by-case basis, and where there exists a particular suspicion. In the aftermath of the September 11, 2001 attacks, the US government determined that PNRs (both archived and real-time) were invaluable tools for investigating and thwarting terrorist attacks. Accordingly, the US government has sought the collection, transfer and retention of PNRs by the US Department of Homeland Security (DHS) Bureau of Customs and Border Protection. In May 2004, the US government negotiated the *2004 Passenger Name Record Data Transfer* agreement (aka. US-EU PNR agreement) – a safe harbor PNR transfer agreement with the European Commission. Specifically, the European Commission deemed that the level of protection afforded to such PNR transfers would satisfy the standard of "adequacy" required by the 1995 EU Data Directive, as long as the data would be transferred and used solely for the purposes for which it was collected. These purposes being limited to "preventing and combating: terrorism and related crimes; other serious crimes, including organized crime, that are trans-national in nature; and flight from warrants or custody for those crimes." The US-EU-PNR agreement required European airlines to supply PNR data to US authorities within 15 minutes of a plane taking off. While this agreement was invalidated by the European Court of Justice in May 30, 2006 due to lack of legal authority, the European Council worked to substantively resurrect the agreement before the court-mandated deadline of September 30, 2006.

[21] *see http://en.wikipedia.org/wiki/Passenger_Name_Record*

	In July 2007, a new, controversial, PNR agreement between the US and the EU was undersigned. A short time afterward, the Bush administration gave exemption for the Department of Homeland Security, for the Arrival and Departure System (ADIS) and for the Automated Target System from the 1974 Privacy Act, raising concerns from Statewatch about the protection of EU citizens' data. In February 2008, Jonathan Faull, the head of the EU's Commission of Home Affairs, complained about the US bilateral policy concerning PNR. The US had signed in February 2008 a memorandum of understanding (MOU) with the Czech Republic in exchange of a VISA waiver scheme, without concerting before with Brussels.[22] The tensions between Washington and Brussels are mainly caused by a lesser level of data protection in the US, especially since foreigners do not benefit from the US Privacy Act of 1974. Data privacy in the EU is regulated by the Directive 95/46/EC on the protection of personal data, and the US Safe Harbor arrangement made to converge with European norms is still being controversed for alleged lack of protection.
Known or potentials dangers /Risks	PNR will typically contain much more information of a sensitive nature. This will include the passenger's full name, date of birth, home and work address, telephone number, e-mail address, credit card details, as well as the names and personal information of emergency contacts. Designed to "facilitate easy global sharing of PNR data," the CRS-GDS companies "function both as data warehouses and data aggregators, and have a relationship to travel data analogous to that of credit bureaus to financial data.". A canceled or completed trip does not erase the record since "copies of the PNRs are 'purged' from live to archival storage systems, and can be retained for months by CRSs, airlines, and travel agencies." Further, CRS-GDS companies maintain web sites that allow almost unrestricted access to PNR data – often, the information is accessible by just the reservation number printed on the ticket. Additionally, "[t]hrough billing, meeting, and discount eligibility codes, PNRs contain detailed information on patterns of association between travelers. PNRs can contain religious meal preferences and special service requests that describe details of physical and medical conditions (e.g., "Uses wheelchair, can control bowels and bladder") – categories of information that have special protected status in the European Union and some other countries as "sensitive" personal data." Thus, PNRs can reveal where you're from, where you went with whom, for how long, and at whose expense. Despite the sensitive character of the information they contain, PNRs are generally not recognized as deserving the same privacy protection afforded to medical and financial records. Instead, they are treated as a form of commercial transaction data. There is no proper control over handling with a PNR transfered to the US Department of Homeland Security (DHS). Report of the The Privacy Office of the U.S. Department of Homeland Security (DHS) of the December 2008 shows a number of major disfunctionalities that proves the DHS did not comply with the EU agreement or with the US legislation in its use of PNR, that includes data from Europeans that travel to US.[23]
Others	Adoption of PNR data transfer agreements shows lack democratic proceedures and oversight. In case of the Czech republic none of the

[22] *see Czech-US visa pact may scupper PNR deal, Commission fears (Europolitics), http://abiweb.obh.hu/dpc/index.php?menu=gyoker/News&dok=Czech-US*
[23] *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf*

	PNR agreement with the US was so far approved by the Czech parliament, transfers are hovewer being carried out. During the preparation of the agreements objections of DPA were routinely ignored.[24]
Generated data bases	
Associated data base/ creation (a line pro database)	From a technical point, there are five parts of a PNR required before the booking can be completed. They are: • The name of the passenger(s). • Contact details for the travel agent or airline office. (While a booking can have more than one contact number, it must have at least one, and it is standard practice for the agency or airline office to be listed first). • Ticketing details, either a ticket number or a ticketing time limit. • Itinerary of at least one segment, which must be the same for all passengers listed. • Name of the person making the booking. Once the booking has been completed to this level, the CRS system will issue a unique alpha-numeric record locator, which will remain the same regardless of any further changes made (except if a multi-person PNR is split). The airline(s) involved will also issue their own references, which will remain as a note in the booking.[25] While the above list is the minimum requirement, there is a considerable amount of other information required by both the airlines and the travel agent to ensure efficient travel. These include: • Fare details, and any restrictions that may apply to the ticket. • The form of payment used, as this will usually restrict any refund if the ticket is not used. • Further contact details, such as agency phone number and address, additional phone contact numbers at passenger address and intended destination. • Age details if it is relevant to the travel, eg, unaccompanied children or elderly passengers requiring assistance. ** this must be added at the time the name is stored during step one above*** • Frequent flyer data. • "Special Service Requests" (SSR) such as special meal requirements, seating preferences, wheelchairs, and other similar requests.

[24] *Czech government accepts the new PNR agreement with reservations, EDRigram 1. August 2007, http://www.edri.org/edrigram/number5.15/czech-pnr-reservations*

[25] *according to wikipedia entry http://en.wikipedia.org/wiki/Passenger_Name_Record*

	• "Optional Services instruction" (OSI), comments which are passed onto the passenger manifest, enabling ground-staff and flight crew to see special information about the passenger such as 'Pilot's Wife' or "Partner VIP" or "The company's CFO must have seat 2A". OSI messages are also used by the airline to re-transmit passenger information back to the booking agent so it is visible to both entities. In more recent times, many governments now require the airline to provide further information included to assist investigators tracing criminals or terrorists. These include: • Passengers' gender • Passport details- nationality, number, and date of expiry. • Date and place of birth. • WatchList exclusion number [26] DHS creates databases of its own from the data on airline passengers transmitted according to EU- USA PNR agreements. DHS retains EU PNR data in an active analytical database for seven years, after which time the data will be moved to dormant, non-operational status. Data in dormant status will be retained for eight years and may be accessed only with approval of a senior DHS official designated by the Secretary of Homeland Security and only in response to an identifiable case, threat, or risk.[27]
What justifies the inscription in the file /Risks?	PNR data serves for booking and other services of airline companies and air ticket dealers companies. Department of Homeland Security (DHS) and U.S. Customs and Border Protection (CBP) declare they are operating Automated Targeting System (ATS) and System of Records Notice (SORN) containing PNR dato to : screen individuals traveling to and from the United States *for the purpose of preventing and combating: (1) terrorism and related crimes; (2) other serious crimes, including organized crime, that are transnational in nature; and (3) flight from warrants or custody for crimes described above. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law.*[28]
Purposes /contents, main data included / Risks?	*See above*
File masters? Risks?	*US* ***Customs and Border Protection and Department of Homeland Security***

[26] *according to wikipedia entry http://en.wikipedia.org/wiki/Passenger_Name_Record*
[27] *Letter from United States to the Council of European Union (2007 Letter), see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf*
[28] *Letter from United States to the Council of European Union (2007 Letter), see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf*

Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of air ticket booking agencies. Broad scale of US security personel - System of Records Notice (SORN) for the Automated Targeting System (ATS)is subject to the Privacy Act of 1974, as amended. ATS is an enforcement screening tool consisting of six separate components, all of which rely substantially on information in the Treasury Enforcement Communications System (TECS). PNR data represents only one of many segments of it.[29]
Data retention delays/ risks Right to be forgotten	See column Associated data base/ creation
Rights to know or to modify data?	„A detailed analysis by the Identity Project in the US shows the specific DHS compliance failings resulted from the report: - Requests for PNR data have typically taken more than a year to answer - many times longer than the legal time limits in the Privacy Act and Freedom of Information Act; - When individuals have requested "all data" about them held by the DHS, often they have not been given any of their PNR data; - Because of this, the vast majority of requesters who should have received PNR data did not; - PNR data has been inconsistently censored before it was released; - A large backlog from the initial requests for PNR data remains unanswered, more than a year later. The results of the report are in line with the findings of the earlier reports of the Identity Project that revealed the practical problems in accessing your PNR data with the DHS. These problems are the same that the European citizens might face in getting access to their data from DHS A clear example is the last year request from MEP Sophia In 't Veld to get her PNR information - a request which received a first false claim from DHS that they didn't have any record of her trip.The MEP finally received her PNR data after EFF lawyers filed a Federal lawsuit on her behalf, but the data was late, clearly incomplete, and inconsistently and inappropriately redacted, according with a well-known PNR expert, Edward Hasbrouck.“[30]
Covert purposes/ Risks/uncontrolled future evolution	US authorities acknowledge they use EU PNR data to profile airline passengers. Mechanisms and impacts of such profiling on rights of the persons affected is unclear. US authorities may share EU PNR data with a third countries “after consideration of the recipient's intended use(s) and ability to protect the information. »[31] EU authorities do not have any possibility to influence such considerations nor effective control mechanisms over the extend, character and purpose of transfer

[29] *Automated Targeting System (ATS) System of Records Notice see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf*

30 DHS Report shows lack of compliance with the EU-US PNR agreement , EDRigram 14. January 2009, http://www.edri.org/edri-gram/number7.1/pnr-dhs-report

[31] *Letter from United States to the Council of European Union (2007 Letter), see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf*

	of EU PNR data to the third countries from the US authorities databases.
Others (interconnections…)	The US programme of PNR data retention and procession inspired some of the goverments of EU member states and European Commission to propose EU-PNR scheme - framework decision. Original proposal was debated by member states, subject to the critical comments of the European Union Fundamental Rights Agency (FRA)[32] and changed into Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes proposed by Council of the European Union on 17 April 2009.[33]
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Czech parliament didnot so far voted for any US EU PNR agreement. Czech government approved the new PNR agreement prepared by the European Commission with the US Department for Homeland Security (DHS) in 2007 with significant reservations.[34]
Risks for freedoms despite the law	EU – US is violating EU data protection regulations according to European Data Protection Supervisor, Peter Hustinx[35] and European Parliament[36]
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Revision of the regulation necessary
Conformity with the European right (Charter of fundamental rights, directives…)	Practice might contravene: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001 and also Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Implementation (or not) of the legislation? / Risks	Being implemented
Others	
This tools and young public or young adults	
How far are young people concerned?	Proportion of youngsters in databases not revealed

[32] *see see PNR: Opinion of the Fundamental Rights Agency http://www.statewatch.org/news/2008/oct/ep-pnr-opinion-fra.pdf*
[33] *see http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf*
[34] *Czech government accepts the new PNR agreement with reservations, EDRigram 1. August 2007, http://www.edri.org/edrigram/number5.15/czech-pnr-reservations*
[35] *see Hustinx letter to the German Council Presidency of 27 June 2007, http://www.statewatch.org/news/2007/jun/eu-us-pnr-hustinx-letter.pdf*
[36] *http://www.statewatch.org/news/2007/jul/04ep-pnr-resolution.htm*

Awareness of issues or of risks	None research done into the issue of awareness of youth in this matter/ Low
Indifference or reaction	None significant reaction
Awareness campaigns/ results	Campaign by Iuridicum Remedium was supported by critical stance of some of the czech parliamentarians towards US - EU PNR agreements and plans of
Good practises	
Campaign to be led. On which themes?	Awareness campaign on risk of uncontrolled proliferation of personal data via PNR systems and agreements
Others	
Conclusions	Practice of the PNR data exchange with the US and adoption of related regulation bypassed in the czech republic democratic legislation process, avoided public debate and expert examination,
Recommendations	According to Peter Hustinx, the European Union's Data Protection Supervisor US EU PNR agreements and practice should be accompanied by guarantees that the individuals whose data are exchanged may examine the exchange process and correct eventual mistakes. US and EU should be allowed to share individual personal data in criminal cases, only if people can take the authorities to court when they are wronged. According to Hustinx : "Strong redress mechanisms, including administrative and judicial remedies, should be available to all individuals, irrespective of their nationality."[37] Possible future EU PNR Framework decision should fulfill recommendation of FRA.[38]

[37] *The EDPS' opinion on the US-EU data exchange agreement, EDRigram of 19. November 2008, http://www.edri.org/edri-gram/number6.22/us-eu-data-edps*

[38] *see PNR: Opinion of the Fundamental Rights Agency http://www.statewatch.org/news/2008/oct/ep-pnr-opinion-fra.pdf*

13 - IN-KARTA

Technology used/tool (For each teams, a card pro tool)	**RFID CARD/ smart – card**
Country/ use area	Czech republic/ Prague
Frame of use	Used as season ticket or **loyalty card** for transport with state owned Czecha railways (České dráhy), ID card and card for free transport for employees of Czech railways, fare fee reduction for student and youngsters, fare fee reduction for pensioners
Population concerned: target and age	General population, users of loyalty discount card
% of users/of young users	Unrevealed
Trends (measured / supposed)	Number of new users in 2007 was 150 000 customers,[39] in April 2009 In-Karta was used by 400000 customers.[40]
Known or potentials dangers /Risks	In 2006 newly established project of In – karta was awarded by negative prize for privacy intrusion in Big Brother Awards contest organised by NGO Iuridicum Remedium.[41] Accorrding to reasoning of the jury Czech railways issued the card only after customers submitted their personal data and then these data were kept in a database of the company related with unique numbers of the card. As a traffic inspectors in each train were equipped with a readers system allowed for tracking of the movement of individual passangers. NGO asked Czech railways to issue anonymous RFID cards and implement measures to prevent tracking the movement of its customers.[42] Czech DPA in its annual report 2008 stated: „According to a plan of inspections inspection of the Czech railways was carried on. Subject of the inspection was processing of personal information in relation to the usage of the new system of fare billing through chip card In-karta. Inspection established that Czech railways intrroduced system of season ticketing using chip cards and violated their responsibility of controller of personal

[39] according to press release of the Czech railways of 2008/02/01, http://www.ceskedrahy.cz/tiskove-centrum/tiskove-zpravy/-2169/
[40] according to press release of the Czech railways of 2009/04/02 http://www.ceskedrahy.cz/tiskove-centrum/tiskove-zpravy/-2698/
[41] see report of Edrigram of 2006/11/08 http://www.edri.org/edrigram/number4.21/bba
[42] press release of NGO Iuridicum Remedium of 2006/10/19
http://www.slidilove.cz/zpravy/nova_in_karta_cd_ma_potencial_narusit_pravo_na_soukromi_milionu_obcanu_v_cr.html_0

	data by not fullfilling their information committments according to § 11 of the act on data protection and by not informing properly holders of the card of the procession of their data. Personal data were processed in contrary to the declare purpose and broader scope, which means processor was not conforming with § 5 art. 1 d)of act on data protection. Inspection established that by processing data collected by In-karta there are collected data on idividual voyages of the travellers which means tracking of the movement of the In-karta holders. With respect to these findings inspector of DPA requested Czech railways to implement changes that will be based on changed rules of processing databases containing information on travelling of the customers. Czech railways informed DPA on 31th. of December 2008 that they fulfilled requested requirements."[43]
Others	Card is currently serving as discount loyalty card in some theatres and since 2008 also as e-purse for rail tickets[44]
Generated data bases	
Associated data base/ creation (a line pro database)	First name, surname, date of birth, place of birht, photograph of the holder face, ID of the card, unique ID of the chip on the card, type of the card, in case of children up to 15 years – name, surname date of birth and adress of their parents, home adress of holder (voluntary), email adress (voluntary), telephone number (voluntary), date of the request, date of issuing the card, signature[45]
What justifies the inscription in the file /Risks?	Processor argues it needs the data for: issuing of the card, and administration of the card and related applications related, Providing of the services for the holder of the card, controll of the authorised use in transport, providing the services of e-purse, protection of the subject from mistake or technological fault during procession and providing of the services, protection of the subject from data theft (!) and prevention of data theft (!), proving of possibility of complains, collecting a data for direct marketing purposes (!)[46]
Purposes /contents, main data included / Risks?	See Known or potentials dangers
File masters? Risks?	Czech railways – controller Other partners of the project – identification of other processors of a data is not possible. Company states it is possible to identify them on the web pages of the project, but there are non mentioned.[47] / From insufficient information on data procession and processors it is impossible for holders to asses the risks related especially with further commercial use of the

[43] Czech Data protection authority Annual Report 2008, pp. 63 - 64, http://www.uoou.cz/files/vz_2008.pdf
[44] for details see english web pages of the project http://www.inkarta.cz/eng-instrukce.aspx
[45] quote from Consent of the client of customers In-karta with procession of personal data, trans. F.P. http://www.inkarta.cz/files/SouhlasOOU-ZIK.pdf
[46] qoute from Consent of the client of customers In-karta with procession of personal data, trans. F.P. http://www.inkarta.cz/files/SouhlasOOU-ZIK.pdf
[47] see http://www.inkarta.cz/

	submitted data by partners of the project, especially in area of direct marketing
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Controller considers all personal information ase confidential and will use them only for declared purposes. Controller will not pass personal data of the subject without its consent to other processors than those binded by a contract.[48] / However purposes of the use of the data are definined very broadly (see What justifies the inscription in the file) and other processors of the data binded by a contract is not possible for the holder to identify (see File masters).
Data retention delays/ risks Right to be forgotten	„Controller declares it will anonymise personal data in its database 5 years after last operation with this electronic financial tool.“[49]
Rights to know or to modify data?	„Subject of a data acknowledges that it can withdraw its consent (with procession of data) through the letter sent to the controller and controller will then liquidate the data... If the subject of the data asks for information on procession of its data or their correction controller is obliged to pass the information or make the change without delay.[50]
Covert purposes/ Risks/uncontrolled future evolution	Hardware of the system and its applications enable covert collection of a data on customers/holders behaviour, habits, usage of services (travelling habits, reading preferencies, etc.). Establishing of universal smart-card in its non-anonymous version forces holders to use services formerly offered on anonymous basis or without massive electronic procession of a data. Free consent of the user with processing his/her data becomes illusionary as the services on anonymous basis are offered for much higher price and/or are not available any more without using of non-anonymous card.
Others (interconnections…)	Complex relations between different data “controllers” and “processors” and complex technical solutions and processes make virtually impossible for user to realise the way it is being dealt with his/her data and asses related risks.
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	No specific legislation on RFID use Personal Data Protection Act, Act 101 of April 4, 2000 Chapter II Rights and obligations in processing of personal data Article 5 (1) The controller shall be obliged to: (a) specify the purpose for which personal data are to be processed;

[48] qoute from Consent of the client of customers In-karta with procession of personal data, trans. F.P. http://www.inkarta.cz/files/SouhlasOOU-ZIK.pdf
[49] quote from conditions of commercial use of In-karta, transl. F.P., http://www.inkarta.cz/files/Obchodni-podminky.pdf
[50] quote from conditions of commercial use, transl. F.P., http://www.inkarta.cz/files/Obchodni-podminky.pdf

	(b) specify the means and manner of personal data processing; (c) process only accurate personal data, which he obtained in accordance with this Act. If necessary, the controller is obliged to update the data. If the controller finds that the data being processed thereby are not accurate with respect to the specified purpose, he takes adequate measures without undue delays, in particular he blocks the processing and corrects or supplements the personal data, or otherwise he must liquidate the personal data. Inaccurate personal data may be processed only within the limits of the provisions of Article 3(6) of this Act. Inaccurate personal data must be branded. The controller is obliged to provide all the recipients with the information about blocking, correction, supplementing or liquidation of personal data without undue delay; (d) collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfilment of the specified purpose; (e) preserve personal data only for a period of time that is necessary for the purpose of their processing. After expiry of this period, personal data may be preserved only for purposes of the state statistical service, and for scientific and archival purposes. When using personal data for these purposes, it is necessary to respect the right to protection of private and personal life of the data subject from unauthorised interference and to make personal data anonymous as soon as possible; (f) process personal data only in accordance with the purpose for which the data were collected. Personal data may be processed for some other purpose only within the limits of the provisions of Article 3(6) or if the data subject granted his consent herewith in advance; (g) collect personal data only in an open manner. Collecting data under the pretext of some other purpose or activity shall be prohibited; (h) ensure that personal data that were obtained for different purposes are not grouped. (2) The controller may process personal data only with the consent of data subject. Without such consent, the controller may process the data: (a) if he is carrying out processing which is essential to comply with legal obligation of the controller; (b) if the processing is essential for fulfilment of a contract to which the data subject is a contracting party or for negotiations on conclusion or alteration of a contract negotiated on the proposal of the data subject; (c) if it is essential for the protection of vitally important interests of the data subject. In this case, the consent of data subject must be obtained without undue delay. If the consent is not granted, the controller must terminate the processing and liquidate the data; (d) in relation to personal data that were lawfully published in accordance with special legislation. However, this shall not prejudice the right to the protection of private and personal life of the data subject, or (e) if it is essential for the protection of rights and legitimate interests of the controller, recipient or other person concerned. However, such personal data processing may not be in contradiction with the right of the data subject

	to protection of his private and personal life. (f) if he provides personal data on a publicly active person, official or employee of public administration that reveals information on their public or administrative activity, their functional or working position, or (g) if the processing relates exclusively to archival purposes pursuant to a special Act. (3) If the controller processes personal data on the basis of a special Act, he shall be obliged to respect the right to protection of private and personal life of the data subject. (4) When giving his consent the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. The controller must be able to prove the consent of data subject to personal data processing during the whole period of processing. (5) If the controller or the processor carries out personal data processing for the purpose of offering business opportunities or services to the data subject, the data subject's name, surname and address may be used for this purpose provided that the data were acquired from a public list or in relation to his activity of controller or processor. The controller or processor, however, may not further process the data specified above if the data subject has expressed his disagreement therewith. The disagreement with processing must be expressed in writing. No additional personal data may be attached to the data specified above without the consent of data subject. (6) The controller who process personal data pursuant to paragraph 5 may transfer these data to some other controller only if the following conditions are met: (a) the data on the data subject were acquired in relation to activities of the controller or the data in question consist in published personal data; (b) the data shall be used exclusively for the purpose of offering business opportunities and services; (c) the data subject has been notified in advance of this procedure of the controller and the data subject has not expressed disagreement with this procedure. (7) Other controller to whom data pursuant to paragraph 6 have been transferred may not transfer these data to any other person. (8) Disagreement with processing pursuant to paragraph 6(c) must be expressed by the data subject in writing. The controller shall be obliged to notify each controller to whom he has transferred the name, surname and address of the data subject of the fact that the data subject has expressed disagreement with the processing. (9) To eliminate the possibility that the name, surname and address of the data subject are repeatedly used for offering business opportunities and services, the controller shall be entitled to further process the subject's name, surname and address in spite of the fact that the data subject expressed his/her disagreement therewith in accordance with paragraph 5. Article 6

	Where authorization does not follow from a legal regulation, the controller must conclude with the processor an agreement on personal data processing. The agreement must be made in writing. In particular, the agreement shall explicitly stipulate the scope, purpose and period of time for which it is concluded and must contain guarantees by the processor related to technical and organisational securing of the protection of personal data. Article 7 The obligations specified in Article 5 shall apply to the processor mutatis mutandis. Article 8 If the processor finds out that the controller breaches the obligations provided by this Act, the processor shall be obliged to notify the controller of this fact without delay and to terminate personal data processing. If he fails to do so, the processor and the data controller shall be liable jointly and severally for any damage incurred by the data subject. This shall in no way prejudice his responsibility pursuant to this Act.
Risks for freedoms despite the law	Complex technical and organisational solution makes very difficult to asses privacy related risks even to experts (DPA) not speaking about common user. Formerly anonymous or semi-anonymous usage of public services is becoming less possible allowing the service providers to track behaviour to track behaviour of the users. Availability of the services is becoming more linked to the assigned electronic (not physical) identity of the user. Loss or damage of an electronic card proving electronic identity might limit access to a citizen to a public services. Leakage of a collected data might further compromise privacy of the user to a third (commercial) parties.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Practice might contravene: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001. Article 5 – Quality of data Personal data undergoing automatic processing shall be: obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; preserved in a form which permits identification of the data subjects for no

	longer than is required for the purpose for which those data are stored. Article 7 – Data security Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. Article 8 – Additional safeguards for the data subject Any person shall be enabled: to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	Create significant part of the users, number not revealed
Awareness of issues or of risks	None research into awareness of the youth on the matter done so far/ Partial
Indifference or reaction	
Awareness campaigns/ results	In 2006 newly established project of In – karta was awarded by negative prize for privacy intrusion in Big Brother Awards contest organised by NGO Iuridicum Remedium. Organisation also sent the letter to the Czech railways requesting introduction of an anonymous card. DPA inspection in 2007 and 2008 resulted in recommedations of modification of databases and results of the inspection were published in Annual report 2008. Czech railways have put partial information on data protection and conditions of data protection to the Consumers contractn and on the web pages of the project.
Good practises	Modification of database according to Czech DPA recommendations

Campaign to be led. On which themes?	Further campaign on introduction of an anonymous card issued at non-discriminatory (pricing) conditions
Others	
Conclusions	Project of the In-karta (smart-card) was introduced without proper assessment of the privacy risks and these risks are not properly analysed even two years after the start of the project. Project meanwhile broadens its scale introduces new services (e-purse).
Recommendations	Establishing a rule of obligatory introducing of anonymous cards instead of non-anonymous cards when possible Establishing a regular privacy assessment procedure (Privacy Impact Assesment) for any project with possible bigger impact on the citizens rights. This might be done by independent auditing organisation, published and submitted to the DPA. Establishing a new legislation specifically focused on RFID.

2-BIOLOGICAL IDENTITY

21 – NATIONAL DNA DATABASE

Technology used/tool (For each teams, a card pro tool)	**DNA ANALYSIS/ DATABASE**
Country/ use area	Czech republic
Frame of use	Database used by Police for identification and investigation purposes
Population concerned: target and age	Persons accused and convicted of committing intentionally criminal act, persons sentenced to compulsory medical treatment
% of users/of young users	Unknown
Trends (measured / supposed)	In march 2009 database contained more than 45 thousands of genetic profiles. Majority of profiles are of sentenced and accused persons, approx 8 thousands are of unidentified profiles from crime scene[51], numbers rised significantly in 2007 after Police and prison authorities was given new authority to collect the data even without a consent of an accused or sentenced citizen by the law no. 321/2006 (resulted in broadscale collection of DNA profiles of inmate population)
Known or potentials dangers /Risks	insufficient legislation, insufficient oversight over security of the data shared and then stored and processed abroad
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	Created since 2002
What justifies the inscription in the file /Risks?	Law on police 273/ 2008, § 65 Gathering of personal information on purposes of future identification provides basic authorisation of the Police, details on operation rules of the database and processing of the data are based on Directive of Police president/ Contravenes recommendation of Council of Europe Committee of ministers Recommendation No. R (92) 1 on the use of analysis of deoxyribonucleic acid within the framework of the criminal justice system
Purposes /contents, main	DNA samples, other personal information of the subjects

[51] *statement of Roman Hradil, deputy chief of department of criminal identification in Criminology Institute in hev, Analýza určí jen rezavé vlasy, in Lidové noviny, 14.3.2009, p. 25*

data included / Risks?	
File masters? Risks?	Criminology institute, Czech Police
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Police experts, access to the files is monitored, deletion can be made by one authorised employee of Criminology institute, DNA profiles are shared with with security services of EU countries and USA but these do not have direct access to the database[52] /access limits regulated by police directives, international agreements – some of them are restricted[53] / no details are available on control and access mechanisms, there are no relevant mechanisms to control use of the data shared with the US institutions[54]
Data retention delays/ risks Right to be forgotten	New police law 273/ 2008 doesnot allow clear interpretation. It is unclear from its § 65 if the Police has to liquidate all the DNA profiles in the database of the persons that have not been accused or sentenced. However the refusal of deletion of such data might contravene art. 8 par.1 of the ECHR as demonstrated in a decision of European court of human rights on 4. 12. 2008. Data of the persons sentenced are stored until they are necessary for prevention, revelation and prosecution of criminal offences or for protection of national security and public order.[55]
Rights to know or to modify data?	Accoding to the old version of the police law, police was obliged to inform the person about processing its genetic data or destroy them after criminal proceeding was finished. However according to the new police law 273/2008 police doesnot have a duty to inform a person about the fact it is processing its data, it must give an information only when the data are deleted. Persons who were not convicted may ask (if they find out their data are stored) deletion of their DNA profiles. Such right was demonstrated in judgements of European court of human rights (30562/04, 30566/04) citing art. 8 par. 1 of the ECHR.
Covert purposes/ Risks/uncontrolled future evolution	Control of the czech DPA revealed in 2008 operation of National database of DNA breaches § 9 of the 101/2000 law on data protection because the data of persons who were not sentenced for serious crimes were stored.[56] New legislation enacted in 2009 further broadens the extend of subjects whos data can be stored in a databases. And there were numerous statements of the police representatives who declared the intention to broaden even more the extend of citizens whose DNA profiles are stored in the database to include for instance military and police personel, firemen etc[57].

[52] *article at web pages of the Czech police http://www.policie.cz/clanek/policie-cr-nezneuziva-dna.aspx*
[53] *Czech-U.S. Agreement on the strengthening of cooperation in the prevention of and the fight against serious crime and Agreement on establishment of anti-terrorist cenre signed in 2008*
[54] *Czech Data protection authority Annual report 2008*
[55] *§ 65 of the police law No. 273/ 2008*
[56] *Czech Data protection authority Annual report 2008*
[57] *see for instance article of police lieutenant of Criminology Institute Radka Šimková, Legislativní problémy národní databáze dna in Kriminalistika 3/2003*

	Subsequent legislation changes also weaked the right of the person to be informed of processing its data and right to seek their deletion.
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Specific legislation is missing, regulated only by directive of police president Applies only law 101/2000 law on data protection and 273/2008 law on police with unclear interpretations. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine[58]
Risks for freedoms despite the law	Contravening art. 8 par. 1 of the ECHR. Article 8 – Right to respect for private and family life 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Necessary adoption of the new legislation acknowledged also in DPA annual report 2008
Conformity with the European right (Charter of fundamental rights, directives…)	Current legislation – directive of police president and 273/2008 law on police are not conforming with art. 8 par. 1 of the ECHR[59]
Implementation (or not) of the legislation? / Risks	Legislation is in early stage of preparation
Others	
This tools and young public or young adults	
How far are young people concerned?	Information on percentage of youngsters DNA profiles in a database is not publicly available
Awareness of issues or of risks	None research made on awareness on the issue among youth, estimated - Low
Indifference or reaction	Indifferent
Awareness campaigns/ results	None
Good practises	None
Campaign to be led. On	Informing youngsters on their rights enshrined in ECHR. Informing

[58] *entered into force in the Czech republic 2001*
[59] *Czech Data protection authority Annual report 2008*

which themes?	youngsters of the meaning and importance of protection of their sensitive biological data and relevance of DNA profiles in that sense
Others	
Conclusions	
Recommendations	Support DPA call for new legislation dealing specifically with DNA databases, establish expert group including privacy experts to start work on new legislation, public awareness campaign

22 -DNA DATABASE : GENOMAC

Technology used/tool (For each teams, a card pro tool)	**DNA ANALYSIS/ DATABASE**
Country/ use area	Czech republic
Frame of use	**Commercial DNA paternity testing,** DNA testing of genetic origin – GenoGraf, establisment of the Czech national genetic database
Population concerned: target and age	Not publicised, in DNA paternity testing included parents with their (presumably) children.
% of users/of young users	Unknown
Trends (measured / supposed)	3000 Czechs agreed that their data are included in database by mid 2007[60], there were 2000 genetic profiles in Czech national genetic database run by the company by march 2008.[61] It is not clear to what extend company also processes DNA data of non-Czech citizens, however it offers its services on the web pages also in Slovak and English languages.[62]
Known or potentials dangers /Risks	Company was fined 90000 Czech crowns after investigation of Czech DPA found out following misconducts: Company have not liquidated personal data nor DNA samples after finishing tests of paternity and genetic origin, documentation contained names, surnames, birth numbers despite the claims of the company it will for research purposes identify clients on by initial letters of their names and specific number of the client. DPA also found out that before the start of the inspection company didnot asked clients for their consent with procession of their data nor their were informed about the extend in which their data will be processed. Company carried on paternity tests and tests of genetic origin without proper registration at the DPA.[63] DPA ordered company to liquidate all personal information processed in violation of law on data protection including DNA profiles and samples.
Others	

[60] *see http://www.genomac.cz/en/view.php?cisloclanku=2007080003*
[61] *press release of the company, see http://scienceworld.cz/biologie/ceska-narodni-genograficka-databaze-spustena-650*
[62] *see http://www.genomac.cz/en/*
[63] *Czech Data protection authority Annual report 2008, http://www.uoou.cz/files/vz_2008.pdf*

Generated data bases	
Associated data base/ creation (a line pro database)	Company was founded in the fall of 2001 and from its early days involved in paternity DNA testing.[64]
What justifies the inscription in the file /Risks?	Person seeking testing sends DNA samples, in case of paternity test also of (presumed) child. / Free consent of a child (or any other second person whos samples are submitted) with procession of his/her data is illusionary
Purposes /contents, main data included / Risks?	DNA samples, other personal information of the subjects
File masters? Risks?	Genomac International, s.r.o./ for risks see Known or potentials dangers
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of the company/ not known/ see Known or potentials danges
Data retention delays/ risks Right to be forgotten	According to the law 101/2000 on data protection controller is obliged to « preserve personal data only for a period of time that is necessary for the purpose of their processing. After expiry of this period, personal data may be preserved only for purposes of the state statistical service, and for scientific and archival purposes. When using personal data for these purposes, it is necessary to respect the right to protection of private and personal life of the data subject from unauthorised interference and to make personal data anonymous as soon as possible.»[65] For information on actual practice see Known or potentials dangers
Rights to know or to modify data?	According to the law 101/2000 on data protection «In collecting personal data the controller shall be obliged to inform the data subject of the scope in which and the purpose for which the personal data shall be processed, who and in what manner will process the personal data and to whom the personal data may be disclosed, unless the data subject is already aware of this information. The controller must inform the data subject about his right of access to personal data, the right to have his personal data rectified as well as other rights provided for in Article 21.»[66] For information on actual practice see Known or potentials dangers
Covert purposes/ Risks/uncontrolled future evolution	see Known or potentials dangers/ risks of possible future genetic discrimination of the subjects whos DNA profiles or samples were compromised
Others	

[64] *web pages of the company http://www.genomac.cz/en/view.php?cisloclanku=2006040002*
[65] *Act no. 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts, art 5, par. e)*
[66] *Act no. 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts, art. 11, par. 1)*

(interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine[67] None specific national legislation with regard to DNA testing and databases.
Risks for freedoms despite the law	
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Necessary adoption of the new legislation acknowledged also in DPA annual report 2008
Conformity with the European right (Charter of fundamental rights, directives…)	
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	Information on percentage of youngsters DNA profiles in a database is not available
Awareness of issues or of risks	None research into the topic done so far, probably low
Indifference or reaction	Indifferent
Awareness campaigns/ results	Press release of the DPA, informing of the public about findings of the inspection,/ not measured, probably influencing practice of other companies providing commercial DNA testing
Good practises	Extensive privacy statement of another company providing commercial DNA testing on the web pages of the company.[68]
Campaign to be led. On which themes?	Informing youngsters of the meaning and importance of protection of their sensitive biological data and relevance of DNA profiles in that sense. Informing adults on the meaning of free consent with processing of the personal data with special relevance to their children, informing on risks of possible genetical discrimination.

[67] *entered into force in the Czech republic 2001*
[68] *http://www.dnatest.cz/cz/15_ochrana_soukromi_zakazniku/cz_privacy.asp#q3*

Others	
Conclusions	
Recommendations	Support DPA call for new legislation dealing specifically with DNA databases, establish expert group including privacy experts to start work on new legislation, public awareness campaign

23 - NATIONAL HEALTHREGISTER

Technology used/tool (For each teams, a card pro tool)	**Databases**
Country/ use area	Czech republic/ Prague
Frame of use	Registers were established with the aim of registering and tracking patients with selected illnesses with serious social impacts, assessing of diagnostic and treatment methods, analysing evolvements, causes and affects of illnesses and statistical health research. The registration in these databases is not at the moment linked to any specific social security benefices for the patients.
Population concerned: target and age	Patients with serious illnesses
% of users/of young users	Unknown
Trends (measured / supposed)	Stagnation of the ammounts of a data[69]
Known or potentials dangers /Risks	„Czech DPA considers problematics of new legal norms related to health registers to be socialy underestimated. Ministry of Health have not accepted request of the DPA to clarify whole concept of the registers. DPA asked for clarification on data retention period in individual registers and explanation why is not (ulike in other EU countries) taken in account consent of the subject of the data. DPA have recommended that in the respect to the extremely sensitive data processed in the registers were those subject of the more detail legislation by the law and not just ministerial decree or Attachement of a legal norm.“[70]
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	National register of inpatients (NRHOSP), National register of women in childbed (NRROD), National register of newborns (NRNAR), National register of congenital defects (NRVV), National register of abortions (NRPOT), National register of physicians, dentists and

[69] from the response of the Institute of Health Information and Statistics of the Czech Republic to the request of Iuridicum Remedium of 2009/5/12

[70] *Czech DPA Annual report 2008, p.91, translation F.P.*

	pharmaceutists (RLZF), National register of users of substitutive drugs (NRUSL), National register of oncological diseases (NOR)[71], National register of vascular surgery (NRCCH)[72], National cardio surgery register (NKCHR)[73], National Register of Joint Replacements (NRKN)[74], National Register of Cardiovascular Interventions (NRKI)[75], National register of occupational deseases (NRNP), National Register of Persons Refusing Donation of Tissues and Organs Posthumously[76], National register of IVF
What justifies the inscription in the file /Risks?	Medical statistics and research, state health policy, illness prevention /see Potential dangers
Purposes /contents, main data included / Risks?	NOR[77] birth number[78], data on treatment and illness of the patient, personal and family anamnesis, data anonymised 25 years afther the death of the patient. NRHOSP birth number, data on treatment and illness of the patient, personal and family anamnesis. Data anonymised 5 years after release from the hospital. NRROD Birht number of a mother, information on pregnancy, the treatment and state of health of mother and newborn baby. Data anonymised 10 years after delivery of a baby. NRNAR Birth numbers of mother and baby, and their health state. Data anonymised 10 years after delivery of a baby. NRVV Birth numbers of mother and baby with congenital defects (NRVV), data on treatment and illness of the child and mother, personal and family anamnesis, data anonymised 5 years after child reaches 15 years of age. RLZF Personal information of physicians, dentists and pharmaceutists. Data anonymised 1 year after finishing of the practice of the medical personel. NRPOT

[71] *http://www.ksrzis.cz/Pages/168-NOR-National-Register-of-Oncological-Diseases.html*
[72] *http://www.ksrzis.cz/Pages/169-NRCCH-National-Register-of-Vascular-Surgery.html*
[73] *http://www.ksrzis.cz/Pages/167-NKR-National-Cardiosurgery-Register.html*
[74] *http://www.ksrzis.cz/Pages/171-NRKN-National-Register-of-Joint-Replacements.html*
[75] *http://www.ksrzis.cz/Pages/170-NRKI-National-Register-of-Cardiovascular-Interventions.html*
[76] *http://www.ksrzis.cz/Pages/173-NROD-National-Register-of-Persons-Refusing-Donation-of-Tissues-and-Organs-Posthumously.html*
[77] *according to Attachement to the Act no. 20/1966 http://www.pravnipredpisy.cz/predpisy/ZAKONY/1966/020966/Sb_020966_------.php*
[78] *unique birth number is given to every newly born citizen(or people who acquire citizenship) according to Register of Population Act and is used as unique identifier for activities of the Ministries, other administrative authorities, bodies entrusted with the performance of State administration and courts, notaries, health insurance companies, etc.*

	Birth number of pregnant woman, personal anamnesis, data on health state of the woman, Data anonymised 10 after abortion. NRCCH Birth number of the patient, data on health state related to the illness, information on the treatment and its results. data anonymised 5 years after the death of the patient. NKCHR Birth number of the patient, data on health state related to the illness, information on the treatment and its results. data anonymised 20 years after the death of the patient. NRKN Birth number of the patient, data on health state related to the illness, information on the treatment and its results. data anonymised 5 years after the death of the patient. NRNP Birth number, date of death, data related to the illness, data related to the occupation of the patient. Data are anonymised 40 let after file is established. NRKI Birth number, health state related to the illness, data on treatment and its results. Data anonymised 5 years after the death of the patient. NRUSL Birth number, nationality, health insurance number, data on health state of the patient and treatment and its results. Data are anonymised 20 years after establishment of the file. National register of IVF Processes only anonymised data of the woman subjected to In vitro fertilisation and anonymised data of the father. Data are submitted by individual medical facilites, data on first name, family name, birth number, date of birth, and permanent adress are submitted from Central register of citizens of Ministry of Interior.
File masters? Risks?	Ústav zdravotnických informací a statistiky České republiky (ÚZIS ČR) – Institute of Health Information and Statistics of the Czech Republic
Who accesses the files/ Sharing of the data base? Access limits? /Risks	«Access to the personal data in the register has processor, controller and relevant medical personell of the medical institution giving treatment to the patient relevant to the register. Relevant medical personell is a person appointed by the director or statutare representative of the medical institution and approved by the

[79] *Act no. 20/1966§ 67 d) art. 8)*

	controller of the register.»[79]
Data retention delays/ risks Right to be forgotten	NOR[80] birth number, data on treatment and illness of the patient, personal and family anamnesis, data anonymised 25 years afther the death of the patient. NRHOSP birth number, data on treatment and illness of the patient, personal and family anamnesis. Data anonymised 5 years after release from the hospital. NRROD Birht number of a mother, information on pregnancy, the treatment and state of health of mother and newborn baby. Data anonymised 10 years after delivery of a baby. NRNAR Birth numbers of mother and baby, and their health state. Data anonymised 10 years after delivery of a baby. NRVV Birth numbers of mother and baby with congenital defects (NRVV), data on treatment and illness of the child and mother, personal and family anamnesis, data anonymised 5 years after child reaches 15 years of age. RLZF Personal information of physicians, dentists and pharmaceutists. Data anonymised 1 year after finishing of the practice of the medical personel. NRPOT Birth number of pregnant woman, personal anamnesis, data on health state of the woman, Data anonymised 10 after abortion. NRCCH Birth number of the patient, data on health state related to the illness, information on the treatment and its results. data anonymised 5 years after the death of the patient. NKCHR Birth number of the patient, data on health state related to the illness, information on the treatment and its results. data anonymised 20 years after the death of the patient. NRKN Birth number of the patient, data on health state related to the illness, information on the treatment and its results. data anonymised 5 years after the death of the patient. NRNP Birth number, date of death, data related to the illness, data related to

[80] *according to Attachement to the Act no. 20/1966 http://www.pravnipredpisy.cz/predpisy/ZAKONY/1966/020966/Sb_020966_------_.php*

	the occupation of the patient. Data are anonymised 40 let after file is established. NRKI Birth number, health state related to the illness, data on treatment and its results. Data anonymised 5 years after the death of the patient. NRUSL Birth number, nationality, health insurance number, data on health state of the patient and treatment and its results. Data are anonymised 20 years after establishment of the file. National register of IVF Processes only anonymised data of the woman subjected to In vitro fertilisation and anonymised data of the father.
Rights to know or to modify data?	Subjects can ask controller (Ministry of health) to clarify on extend of their personal data processed. Specific information on content of a data they can obtain only from medical facility that submitted the data to the register.[81] Information on these rights are not publicly available to the subjects.
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	defined by Act no. 20/1966 Sb. on National Health Care, in wording of later amendments - §67c., Act no. 89/1995 Sb. on State Statistical Service, in wording of later amendments., Act no. 101/2000 Sb. on Personal Data Protection, in wording of later amendments,/ Ordinance of Ministry of health no. 552/2004 on transfer of the personal and other data into National health information system for the purpose of National health registers (Vyhláška č. 552/2004 Sb., o předávání osobních a dalších údajů do Národního zdravotnického informačního systému pro potřeby vedení národních zdravotních registrů.)/ Mandatory instructions of National Health Information Systems (Závazné pokyny NZIS)
Risks for freedoms despite the law	
If revision of the regulation: reasons?	

[81] from the response of the Institute of Health Information and Statistics of the Czech Republic to the request of Iuridicum Remedium of 2009/5/12

Result: improvement or aggravation (compared to the protection of the DP)	
Conformity with the European right (Charter of fundamental rights, directives…)	Might contravene : Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Applies also: Position No. 3/2004 Personal Data Processing in the Context of Clinical Testing of Drugs and Other Medical Substances[82]
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	Number of youngsters among subjects of a data not revealed by the Institute of Health Information and Statistics [83]
Awareness of issues or of risks	None research made so far, probably very low
Indifference or reaction	None
Awareness campaigns/ results	None
Good practises	None
Campaign to be led. On which themes?	Awareness campaign on extend of data currently processed, importance of free consent with data protection and legislation change
Others	
Conclusions	
Recommendations	Clarification of a concept of the registers. Inclusion of free consent of the patient with the procession of the data. Shortening of the data retention periods. For more see Czech DPA recommendations in Known or potentials dangers.[84]

[82] http://www.uoou.cz/index.php?l=en&m=left&mid=02:109&u1=&u2=&t=

[83] from the response of the Institute of Health Information and Statistics of the Czech Republic to the request of Iuridicum Remedium of 2009/5/12

[84] *Czech DPA Annual report 2008, p.91, translation F.P.*

24 - CENTRAL REPOSITORY OF ELECTRONIC PRESCRIPTIONS

Technology used/tool (For each teams, a card pro tool)	**Database**
Country/ use area	Czech republic/ Prague
Frame of use	Repository was established for the collection and processing of electronically prescribed medicinal products[85] but is being used also for control of distribution and use of the medicinal products, "OTC medicinal products subject to sales restriction» - which contain some active substances which can be missused narcotic at illegal drug market ,[86] and for processing of information on prescription of pharmaceuticals to individuals
Population concerned: target and age	Patients using electronic prescription, patients using certain drugs for flu or pain killers, generally all individuals using pharmaceuticals
% of users/of young users	Not revealed
Trends (measured / supposed)	Central repository was established by the end of 2008,[87] data started to be collected by May 2009, amount of data processed and stored rapidly grow since than, in July 2009 data on medication of the 200 000 patients were daily submited to the database[88]
Known or potentials dangers /Risks	Repository was created by the law to collect and process data on electronic prescription of the drugs, however in 2009 State Institute for Drug Control (SÚKL) started to request pharmacies to ask in the repository whether specific patient have recieved medical products subjected to sales restrictions, Pharmacies are also requested to submit to the central repository data on distributed pharmaceuticals to individual patients, this is being done without detail legislation by law just on the basis of Direction LEK 13[89] issued by the State

[85] Act No 378/2007 Coll., on Pharmaceuticals and on Amendments to Some Related Acts, Section 81, see http://www.sukl.cz/uploads/Legislativa/Zakon_o_lecivech_EN_corr_clean2.pdf

[86] *State Institute for Drug Control: INFORMATION FOR MARKETING AUTHORISATION HOLDERS, http://www.sukl.cz/uploads/Registrace/OTC_s_omezenim/OTC_o_omez_drzitele_EN.pdf*

[87] *Jaromír Weber : SUKL rekapituloval, in Medical Tribune, 2009/01/06, p 7*

[88] Veronika Rodriguez: Office collects sensitive data that can be easily misused (Úřad sbírá citlivá data, která se dají lehce zneužít), in Aktualne.cz, 2009/06/06, http://aktualne.centrum.cz/domaci/zivot-v-cesku/clanek.phtml?id=639077

[89] http://www.sukl.cz/lek-13-verze-1?lred=1

	Institute for Drug Control. Patients are not asked for their consent with procession of their seinsitive nor properly informed on the extend of the processing of their data.[90] SÚKL has already announced a plan to establish till the end of 2009 online application that would anable patients to enter through using of specific code information on the medication they were subscribed by the physicians and sold by pharmaceutists and history of their drug taking.[91] Some of the media also raised concerns over the fact that software solutions, procession and coding of the data is subcontracted to the private companies. Some of the has the links on commercial health insurance companies.[92] In August 2009 Czech DPA stated that creation of database was illegal and ordered deletion of collected personal and sensitive data.[93]
Others	At the moment new legislation (amendment of Act on Pharmaceuticals) is being prepared by the Ministry of health to allow for re-creation of central repository, this time on legal basis.
Generated data bases	
Associated data base/ creation (a line pro database)	Central repository of electronic prescriptions
What justifies the inscription in the file /Risks?	Electronic prescription of pharmaceuticals, state health policy/ Disclosure of sensitive data of the patients, misuse of the data by commercial health insurance companies, discrimination in access to the medical treatment
Purposes /contents, main data included / Risks?	**Section 81** **Central repository of electronic prescriptions** The central repository of electronic prescriptions shall be established by the Institute as its organisational part to ensure the fulfilment of the following tasks: a) to accept and collect electronic prescriptions sent by prescribing doctors; b) to notify the doctor immediately after the receipt of the electronic prescription of the identification code for the prescription on the basis of which the prescribed medicinal products will be dispensed in the pharmacy;

[90] *Commentary of the Czech association of pharmaceutists to the system of the electronic prescription, obligation to pass information on distributed medical substances and accounting of the distributed medical substances with pseudoefedrin of the 4. 5. 2009, http://www.lekarnici.cz/download/pro-nepriblasene/sukl/Komentar%20CDu.pdf*

[91] Václav Pergl : Patients will have their own record on pharmaceuticals (Pacient bude mít vlastní lékový záznam), in Právo, 2009/06/03, p. 19

[92] *Veronika Rodriguez: Office collects sensitive data that can be easily misused (Úřad sbírá citlivá data, která se dají lehce zneužít), in Aktualne.cz, 2009/06/06, http://aktualne.centrum.cz/domaci/zivot-v-cesku/clanek.phtml?id=639077*

[93] *see Collection of Czech patients' sensitive data illegal – office, http://www.ceskenoviny.cz/zpravy/collection-of-czech-patients-sensitive-data-illegal-office/391294&id_seznam=19530*

	c) to provide free-of-charge access to the electronic prescription on the basis of which the medicinal products is to be dispensed to the pharmacist dispensing medicinal products in the concerned pharmacy immediately after the receipt of his or her request; d) to ensure a continuous, free-of-charge access to the database of electronic prescriptions for prescribing doctors and pharmacists dispensing prescribed medicinal products in pharmacies; e) to ensure that electronic prescriptions in the database of stored electronic prescriptions are safe and protected from damage, abuse or loss pursuant to a special legal regulation36); f) to ensure the protection and handover of data in the case of terminating operation; g) to immediately label the electronic prescription made available pursuant to letter (c) and issued pursuant to Section 82.[94]/ Main data include : number of health insurance (birth number or date of birth name), code of medication, amount of medication, price by manufacturer, payment by health insurance company, batch of medication, ID of physician subscribing medication, ID of pharmacy.[95]/ For risks see above
File masters? Risks?	Státní Ústav pro kontrolu léčiv (SÚKL) State Institute for Drug Control / part of the data processing is being subcontracted – outsourced to private companies with links to health insurance companies
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Detail information on right to the acces to the files are not available, data are accessed by personel of SÚKL and pharmaceutists.
Data retention delays/ risks Right to be forgotten	Not revealed
Rights to know or to modify data?	Unclear
Covert purposes/ Risks/uncontrolled future evolution	See Known or potentials dangers /Risks
Others (interconnections…)	

[94] *Act No 378/2007 Coll., on Pharmaceuticals and on Amendments to Some Related Acts*
[95] *Veronika Rodriguez: Office collects sensitive data that can be easily misused (Úřad sbírá citlivá data, která se dají lehce zneužít), in Aktualne.cz, 2009/06/06*

Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Act No 378/2007 Coll., on Pharmaceuticals and on Amendments to Some Related Acts[96], Direction LEK 13[97] issued by the State Institute for Drug Control.
Risks for freedoms despite the law	See Known or potentials dangers/Risks
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Revision of the legislation (ongoing) might result due to pressure of Ministry of Health in adoption of special legislation that will seek exemptions from provisions and principles of data protection legislation.
Conformity with the European right (Charter of fundamental rights, directives…)	Might contravene : Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001, Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Applies also: Position No. 3/2004 Personal Data Processing in the Context of Clinical Testing of Drugs and Other Medical Substances[98]
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	Number of youngsters among subjects of a data not revealed by the Institute.
Awareness of issues or of risks	None research made so far, relatively low despite high publicity of the recent DPA ruling.
Indifference or reaction	None
Awareness campaigns/ results	None
Good practises	None
Campaign to be led. On	Awareness campaign on principles of data protection and their relation with special legislation under preparation, importance of free

[96] see http://www.sukl.cz/uploads/Legislativa/Zakon_o_lecivech_EN_corr_clean2.pdf

[97] *see http://www.sukl.cz/lek-13-verze-1?lred=1*

[98] *http://www.uoou.cz/index.php?l=en&m=left&mid=02:109&u1=&u2=&t=*

which themes?	consent with data protection
Others	
Conclusions	
Recommendations	Clarification of a concept of the central repository. Inclusion of free consent of the patient with the procession of the data. Defining of the data retention periods. Legislation change. Campaign raising awareness with risks related with procession of sensitive information for health specialists as well as for broader public

3-INTERPERSONAL COMMUNICATIONS

31 - RETENTION OF DATA ON ELECTRONIC COMMUNICATION

Technology used/tool (For each teams, a card pro tool)	**Retention of a data on electronic communication**
Country/ use area	Czech republic/
Frame of use	On 1 September 2008, the amendment to Act No. 127/2005 Coll., on Electronic Communications entered into force, which completed implementation of the European Directive on Data Retention[99]. Latest amendment includes obligation to retain operational and localisation data of unsuccessful calls in both fixed and mobile telephone networks. Obligation to archive the mentioned data of unsuccessful telephone calls is effective since 2005 already.[100]
Population concerned: target and age	General population, users of electronic communication (mobile phones, land line, emails etc.)
% of users/of young users	Unknown
Trends (measured / supposed)	**EXTEND OF** DATA stored in databases created since 2006 is not revealed. According to the data of Czech police it have used location and traffic data in 35300 cases in 2007.[101] New proposal of Ordinance of the Ministry if Industry and Trade defines extend of the collected data. These include data as defined in European Directive on Data retention and above that: pre-paid phone card identificator and other data related to its use, public phone box identification (number and geographic position data), IP adresses of terminals from which were sent SMS (service od sending SMS from web form, quite widespread service in the Czech Rep.), every link between MSISDN and IMEI used together in the network,. ID of mobile phone credit coupon and its link to mobile phone number (at anonymous SIMs), "additional information" not more specified, with the email and internet communication, use of secured communication, identificator of user´s device, status of event (e.g.fail/success, usual/unusual termination of connection),"identificators of interest" (except IP adress is named as example port number), method and status requests for service, transport protocols etc. New Ordinance also

[99] see Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

[100] see document of Ministry of Industry and Trade : Operational and Localisation Data Retention, 2008/09/25, http://www.mpo.cz/dokument50249.html

[101] Response of press department of the Czech police presidium of 2008/01/31 to the request of Filip Pospíšil

	proposes data retention period of 6 months. New Ordinance was due to take effect from September 2009 but was postponed.[102] For overview of current practice on data retention in the Czech republic see Overview of national data retention policies by AK Vorrat.[103]
Known or potentials dangers /Risks	"Traffic data retention interferes with the fundamental right to confidential communications guaranteed to the individuals by Article 8 of the European Convention on Human Rights. In a democratic society, any interference with this fundamental right can be justified if it is necessary in the interests of national security. It can ultimately result in keeping track of and charting all contacts and relationships held by individuals as well as the places in which this happens and the means used for such purposes The European Court of Human Rights has also stressed that secret surveillance poses a danger of undermining or even destroying democracy on the ground of defending it; additionally, the Court has affirmed that States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[104] For detail legal analysis see also study of Francesca Bignami.[105]
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	Databases of electronic communications services' providers
What justifies the inscription in the file /Risks?	Billing purposes of the telecommunication and internet service providing companies and Act No. 127/2005 Coll. on Electronic Communications in the wording of its later amendments,
Purposes /contents, main data included / Risks?	Billing purposes of ISP and telecommunication companies, purposes of investigation, detection and prosecution of serious crime by national authorities./ see Article 5 of Data retention directive[106] and column Trends (measured / supposed) of this table
File masters? Risks?	ISPs and telecommunication providers
Who accesses the	Data are transferred on the request of the authorised department of

[102] *see proposal of the Ordinance at web pages of the Czech Chamber of Commerce, http://www.komora.cz/hk-cr-top-02-sede/podpora-podnikani-v-cr/pripominkovani-legislativy/art_29852/88-09-navrh-vyhlasky-o-uchovavani-a-predavani-provoznich-a-lokalizacnich-udaju-t-15-5-2009.aspx*

[103] *http://wiki.vorratsdatenspeicherung.de/Overview_of_national_data_retention_policies*

[104] *see Opinion of Article 29 Data Protection Working Party 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), adopted on 21st October 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf*

[105] ***Bignami, Francesca E. (2007)*** *Privacy and Law Enforcement in the European Union: The Data Retention Directive. Chicago Journal of International Law, 8 . pp. 233-255.*

http://eprints.law.duke.edu/1602/1/8_Chi._J.__Int%27l_L._233_(2007).pdf

[106] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT*

files/ Sharing of the data base? Access limits? /Risks	Police in electronical form. Some details are set in Ordinance 285/2005 of Ministry of Informatics and Ministry of Interior / Security arrangements of providers and Police are not revealed/impossible to asses
Data retention delays/ risks Right to be forgotten	New proposal of Ordinance of the Ministry if Industry and Trade defines as general retention period 6 months, data that were passed on authorised national security personell and data on connections between telephone numbers and identifiers of the user are to be stored by providers for 12 months.[107]
Rights to know or to modify data?	Regarding the data passed onto the Police applies regulation of the § 83 of new Police act.[108] It provides for the right of a citizen to be informed within 60 days after submitting of written request about the data police collects or processes on him. Police has also to delete, modify or block inaccurate, wrong data upon the request. These rights will not apply in broadly defined cases when police considers submitting of such information would jeopardize prevention, investigation of criminal offences and protection of the security and public order, jeopardize state secrets or interests of the third persons.
Covert purposes/ Risks/uncontrolled future evolution	Information stored by providers police already uses in investigation of the minor offences according to the information of the czech lawyers. In the 2008 the Electronic Communications Act was amended in a way that left a backdoor for intelligence services to use the providers databases.[109]
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Act No. 127/2005 Coll., on Electronic Communications and its amendments, Ordinance 285/2005 of Ministry of Informatics and Ministry of Interior,
Risks for freedoms despite the law	See column Known or potentials dangers /Risks
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Iuridicum Remedium together with two law offices prepared a issue to the Constitutional Court of the Czech Republic and is currently collecting signatures of 41 parliamentarians necessary for submitting of the challenge. Constitutional challenge seeks abolition of data retention provisions in Act on Electronic Communications.

[107] *see proposal of the Ordinance at web pages of the Czech Chamber of Commerce, http://www.komora.cz/hk-cr-top-02-sede/podpora-podnikani-v-cr/pripominkovani-legislativy/art_29852/88-09-navrh-vyhlasky-o-uchovavani-a-predavani-provoznich-a-lokalizacnich-udaju-t-15-5-2009.aspx*

[108] Act *No.* 273/2008 *Coll., on the* Police *of the Czech Republic, http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=273&PC_8411_p=83&PC_8411_name=o%20policii&PC_8411_l=273/2008&PC_8411_ps=10#10821*

[109] see *Czech Parliament - close in implementing data retention directive in Edrigram of 2008/06/04, http://www.edri.org/edrigram/number6.11/czech-data-retention*

Conformity with the European right (Charter of fundamental rights, directives…)	Procession of the data probably not meeting european standards set by: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001. Data retention directive is currently constitutionaly challenged in several countries. In Germany Administrative Court of Wiesbaden found alreday the blanket recording of the entire population's traffic data on telephone, mobile phone, e-mail and Internet usage is disproportionate.[110] In the Czech republic NGO Iuridicum Remedium is collecting signatures of the parliamentarians for challenge at the Czech Constitutional Court.
Implementation (or not) of the legislation? / Risks	Legislation is being implemented
Others	
This tools and young public or young adults	
How far are young people concerned?	Data not available
Awareness of issues or of risks	None public opinion research into this matter done so far
Indifference or reaction	None
Awareness campaigns/ results	Czech NGO has publicised several articles and also established web pages informing of the risks of unlimited collection of communication data. It has also several time approached members of EP and Czech parliament with a letters asking amendments of the legislation in an attempt to ensure more balanced approach towards the data protection.[111]
Good practises	See chapter Awareness campaigns
Campaign to be led. On which themes?	Awareness campaign on fundamental right to confidential communications guaranteed to the individuals by Article 8 of the European Convention on Human Rights, awareness campaign on actual practice and extend of a traffic and location data stored by ISP and telecommunication providers and transfered to the Police.
Others	

110 see Germany: Data retention is disproportionate, Edrigram 2009/03/25, http://www.edri.org/edri-gram/number7.6/data-retention-court-case-germany

[111] for details see web pages of the campaign of Iuridicum Remedium http://www.slidilove.cz/kampan/16/data_retention.html, Czech Parliament - close in implementing data retention directive in Edrigram of 2008/06/04, http://www.edri.org/edrigram/number6.11/czech-data-retention

Conclusions	
Recommendations	The issue of data retention should be a subject of broader public discussion which was so far avoided in the national context. Constitutionality of the provisions and practice of the data retention should be assessed by Constitutional court.

4-SOCIAL NETWORKS AND NEW GATE KEEPERS OF COMMUNICATIONS

41 - LIDE.CZ

Technology used/tool (For each teams, a card pro tool)	Social network
Country/ use area	Czech republic/
Frame of use	Lide.cz (means people.cz) free-access social networking website that is operated and privately owned by Seznam.cz, a.s. Users can join networks organized by type of activities (chats, discussion fora, blogs,online dating) topics, interests, etc to connect and interact with other people. People can also add friends and send them messages, and update their personal profiles to notify friends about themselves.
Population concerned: target and age	In February 2009 service lide.cz was second most popular social network in the Czech republic used by 20 percent of the internet users.[112] According to the statistics of Seznam.cz and NetMonitor from April 2009 there were 1 705 778 real users a month[113] of which 28.41 percent of the users were 12 -19 years old, 25.76 percent 20 - 29 years old.[114] According to the most recent statistics lide.cz has 420 445 visitors per day in October 2009.[115]
% of users/of young users	See above
Trends (measured / supposed)	Slow growth of the numbers of the users in past half a year according to the data of the independent research project Net monitor.[116]
Known or potentials dangers /Risks	There were recently media reports on misuse of personal information submitted by the users for cyber bulling, black mailing and even physical assults on the girls.[117] According to the executive director of Seznam.cz Pavel Zima, company also sends to the Czech police every week two or three denouncements on possible paedophiles.[118] Despite the fact there has been recently some public discussions on the risks related to the misuse of posted data on the internet (for instance for profiling candidates for employment by companies)[119], many of the users are still ignoring

[112] *Facebook na místní servery stále nestačí,in ct24.cz of 2009/02/03, http://www.ct24.cz/media/44429-facebook-na-mistni-servery-stale-nestaci/*
[113] *see statistics of company Seznam.cz at http://onas.seznam.cz/cz/reklama/nase-internetove-servery*
[114] *statistics of Seznam.cz and NetMonitor, http://onas.szn.cz/onas/beta.onas.test/OUTPUT/NetMonitor/lide_cz/lide.cz.pdf?2009-06-10*
[115] *see statistics of company Seznam.cz at http://onas.seznam.cz/cz/reklama/nase-internetove-servery/*
[116] *for detail see http://www.netmonitor.cz/*
[117] *Vladimír Rogl: ZNEUŽITÍ INTERNETU (Misuse of the Internet) in Slánské listy, 2009/04/28, p. 17,*
[118] *Dění na Internetu, in Lupa.cz of 2009/02/12, http://www.lupa.cz/clanky/seznam-v-roce-vnitrni-konsolidace/*

119 45% zaměstnavatelů lustruje své potenciální zaměstnance přes sociální sítě in http://www.tyinternety.cz/socialni-site/45-zamestnavatelu-lustruje-sve-potencialni-zamestnance-pres-socialni-site-195 reffering to the report Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds,

	possible risks.
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	Data submitted by the users and collected by Seznam.cz.[120]
What justifies the inscription in the file /Risks?	Consent of the user with Licence agreement of Seznam.cz/ However in this agreement it is not defined how will be data further processed and stored. Company Seznam.cz there only states: «Operator declares it feels covenant not to pass information on the content of the email messages (accepted, drafted or sent) onto a third person, it will not edit, censor or monitor them with the excemption of monitoring of the number of messages user receives and sends and systematic monitoring of the content of the emails by antispam and antivirus software.»[121]
Purposes /contents, main data included / Risks?	Purpose of the service is to offer a platform for electronic sharing of personal data and social contacts. It is also used for advertising and marketing purposes. / Data collected include: name, email address, telephone number, address, gender, schools attended, year of school education, and other personal (photographs, movies, messages) or preference information (links, friends links). Extend to which Seznam.cz also collects information on browser type and IP address of the user, certain information from browsers using 'cookies' is unclear./ for Risks see Known or potentials dangers
File masters? Risks?	Data submitted by users, processor of the data is company Seznam.cz
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Access to the file is restricted by simple login, part to the data (gender, age, name) available to everyone, other just to approved «friends»
Data retention delays/ risks Right to be forgotten	Unclear – according to the Licence agreement of Seznam.cz user can cansel his/her account it is unclaer however from the agreement what will happen with collected data. Wording of the Licence agreement also provides for censorship of improper content by the operator.[122]
Rights to know or to modify data?	See Data retention delays/ risks/ Right to be forgotten
Covert purposes/ Risks/uncontrolled	

http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&cbsid=6e63b1d67ff8402bb65ce9ac927cab03-313226522-wt-6

[120] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*
[121] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*
[122] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*

future evolution	
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	None specific national legislation adopted, EU DP directives applies however there is lack of enforcement of those directives in the case of social network.
Risks for freedoms despite the law	Data included in social network database can be misused for profiling, collecting of personal informations by third parties, discrimination etc.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Procession of the data probably not meeting european standards set by: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001.
Implementation (or not) of the legislation? / Risks	There was not any result of investigation into conformity of the practice of social networks with DP legislation published by the DPA, nor position of DPA issued on this matter.
Others	
This tools and young public or young adults	
How far are young people concerned?	See % of users/of young users
Awareness of issues or of risks	More general research on awareness of the children about the risks on the internet and behaviour of the children related to internet was publicised in May 2009. From the results: Czech children on average spend on the Internet 12 hours a week. More than one-third of children aged 14-15 provide unknown people with their personal and contact data through the Internet. 17 percent of parents pay no interest to what their children actually do

	when they use the Internet, though most parents control their children at least from time to time. Only 8 percent of parents use special programmes limiting children's access to unsuitable Internet pages. 51 percent of children aged 10 – 15 years has computer with internet in their children room. About 70 percent of the children aged 14-15 visits discussion groups on the internet 93 percent of children aged 10-11 let downloads and play online games More than a third of the children aged 14 – 15 years shares their personal data with unknown people on the internet 45 percent of the children aged 14 – 15 years shares their photographs and videos on the internet[123]
Indifference or reaction	None
Awareness campaigns/ results	Seznam.cz announced in June 2009 it produced an educational film for young users (12 – 16 years) on services Spoluzaci.cz and Lide.cz. Film is to present the risks of social networks especially related to misuse of networks by paedophiles. Company has also announced a plan to introduce from 2010 registration of the profiles through the SMS. According to product manager of social networks at Seznam.cz the measure is intended to limit a number of short term used profiles. "Up to 8 thousands of such profiles is created daily and part of them might be misused against children," said product manager Martin Kožíšek.[124] Seznam.cz also runs web pages Get acquinted safely[125] containing awareness materials on internet safety including films and Decalogue of internet safety, reporting button for internet abuse. However these pages contain very limited information on the way company itself deals with the data of the users. Several czech NGOs run awareness campaigns on the risks children face on the internet and offer also advices for safe behaviour and safety measures for both parents and children. Several web portals and help lines for referring of online abuse of a children were established. [126] Czech DPA created special web page advising principles and practical steps for securing childrens privacy online.[127] Special chapter in an online toolkit on protection of privacy in social networks was set up by NGO Iuridicum Remedium in May 2009.[128] During its European Presidency Czech government organised ministerial conference Safer Internet for Children where so called Pragues declaration was adopted.[129]

[123] *TNS AISA agency conducted its poll among pupils and students of basic and secondary schools and their parents in January 2009. The pollsters addressed 600 families and 319 of them returned the filled in questionnaires designed for children and especially for their parents to the pollsters, see http://www.ceskenoviny.cz/tema/index_view.php?id=378271&id_seznam=2058*

[124] *Dominik Hrodek: Seznam natočil výchovný film, in Strategie, 2009/06/01, p.10*
[125] *http://www.seznamsebezpecne.cz/*
[126] *see for instance: http://www.saferinternet.cz/, http://www.internethotline.cz/, http://www.internethelpline.cz/*
[127] *see http://www.uoou.cz/uoou.aspx?menu=287&submenu=335*
[128] *see http://www.uzijsisoukromi.cz/socialni-site/*
[129] *for Pragues declaration and presentations at the conference see http://www.mvcr.cz/mvcren/article/participants-of-the-conference-safer-internet-for-children-adopted-the-prague-declaration.aspx*

Good practises	See chapter Awareness campaigns
Campaign to be led. On which themes?	Awareness campaign on rights of the users of the social networks and implementation of better privacy protection practices by Seznam.cz, better informing on the way how company processes personal data.
Others	
Conclusions	
Recommendations	Agreement on social networking of the youth reached between European Commission and 17 companies operating social networks has show possibility of elevating of the levels of the privacy arrangements of the networks through public and political pressure. However measures introduced are still not satisfactory and they do not also apply to the adult users. Special focus need to be given to the practice of retaining of a data even from cancelled profiles and rules of transfer and procession of a data by a third parties (government bodies, other service providers, marketing and advertising companies). Companies providing service of social networks has also to adopt transparent information policy on the way they process or share data of the users.

42 - LIBIMSETI.CZ

Country/ use area	Czech republic/
Frame of use	Lide.cz (means people.cz) free-access social networking website that is operated and privately owned by Seznam.cz, a.s. Users can join networks organized by type of activities (chats, discussion fora, blogs,online dating) topics, interests, etc to connect and interact with other people. People can also add friends and send them messages, and update their personal profiles to notify friends about themselves.
Population concerned: target and age	In February 2009 service lide.cz was second most popular social network in the Czech republic used by 20 percent of the internet users.[130] According to the statistics of Seznam.cz and NetMonitor from April 2009 there were 1 705 778 real users a month[131] of which 28.41 percent of the users were 12 -19 years old, 25.76 percent 20 - 29 years old.[132] According to the most recent statistics lide.cz has 420 445 visitors per day in October 2009.[133]
% of users/of young users	See above
Trends (measured / supposed)	Slow growth of the numbers of the users in past half a year according to the data of the independent research project Net monitor.[134]
Known or potentials dangers /Risks	There were recently media reports on misuse of personal information submitted by the users for cyber bulling, black mailing and even physical assults on the girls.[135] According to the executive director of Seznam.cz Pavel Zima, company also sends to the Czech police every week two or three denouncements on possible paedophiles.[136] Despite the fact there has been recently some public discussions on the risks related to the misuse of posted data on the internet (for instance for profiling candidates for employment by companies)[137], many of the users are still ignoring possible risks.
Others	
Generated data	

[130] *Facebook na místní servery stále nestačí,in ct24.cz of 2009/02/03, http://www.ct24.cz/media/44429-facebook-na-mistni-servery-stale-nestaci/*
[131] *see statistics of company Seznam.cz at http://onas.seznam.cz/cz/reklama/nase-internetove-servery*
[132] *statistics of Seznam.cz and NetMonitor, http://onas.szn.cz/onas/beta.onas.test/OUTPUT/NetMonitor/lide_cz/lide.cz.pdf?2009-06-10*
[133] *see statistics of company Seznam.cz at http://onas.seznam.cz/cz/reklama/nase-internetove-servery/*
[134] *for detail see http://www.netmonitor.cz/*
[135] *Vladimír Rogl: ZNEUŽITÍ INTERNETU (Misuse of the Internet) in Slánské listy, 2009/04/28, p. 17,*
[136] *Dění na Internetu, in Lupa.cz of 2009/02/12, http://www.lupa.cz/clanky/seznam-v-roce-vnitrni-konsolidace/*

137 45% zaměstnavatelů lustruje své potenciální zaměstnance přes sociální sítě in http://www.tyinternety.cz/socialni-site/45-zamestnavatelu-lustruje-sve-potencialni-zamestnance-pres-socialni-site-195 ***reffering to the report Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds, http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&cbsid=6e63b1d67ff8402bb65ce9ac927cab03-313226522-wt-6***

bases	
Associated data base/ creation (a line pro database)	Data submitted by the users and collected by Seznam.cz.[138]
What justifies the inscription in the file /Risks?	Consent of the user with Licence agreement of Seznam.cz/ However in this agreement it is not defined how will be data further processed and stored. Company Seznam.cz there only states: «Operator declares it feels covenant not to pass information on the content of the email messages (accepted, drafted or sent) onto a third person, it will not edit, censor or monitor them with the exception of monitoring of the number of messages user receives and sends and systematic monitoring of the content of the emails by antispam and antivirus software.»[139]
Purposes /contents, main data included / Risks?	Purpose of the service is to offer a platform for electronic sharing of personal data and social contacts. It is also used for advertising and marketing purposes. / Data collected include: name, email address, telephone number, address, gender, schools attended, year of school education, and other personal (photographs, movies, messages) or preference information (links, friends links). Extend to which Seznam.cz also collects information on browser type and IP address of the user, certain information from browsers using 'cookies' is unclear./ for Risks see Known or potentials dangers
File masters? Risks?	Data submitted by users, processor of the data is company Seznam.cz
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Access to the file is restricted by simple login, part to the data (gender, age, name) available to everyone, other just to approved «friends»
Data retention delays/ risks Right to be forgotten	Unclear – according to the Licence agreement of Seznam.cz user can cansel his/her account it is unclaer however from the agreement what will happen with collected data. Wording of the Licence agreement also provides for censorship of improper content by the operator.[140]
Rights to know or to modify data?	See Data retention delays/ risks/ Right to be forgotten
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections…)	
Legislation in	

[138] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*
[139] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*
[140] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*

application	
Law /rules / others (?) (implemented for this data base or this technology)	None specific national legislation adopted, EU DP directives applies however there is lack of enforcement of those directives in the case of social network.
Risks for freedoms despite the law	Data included in social network database can be misused for profiling, collecting of personal informations by third parties, discrimination etc.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Procession of the data probably not meeting european standards set by: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001.
Implementation (or not) of the legislation? / Risks	There was not any result of investigation into conformity of the practice of social networks with DP legislation published by the DPA, nor position of DPA issued on this matter.
Others	
This tools and young public or young adults	
How far are young people concerned?	See % of users/of young users
Awareness of issues or of risks	More general research on awareness of the children about the risks on the internet and behaviour of the children related to internet was publicised in May 2009. From the results: Czech children on average spend on the Internet 12 hours a week. More than one-third of children aged 14-15 provide unknown people with their personal and contact data through the Internet. 17 percent of parents pay no interest to what their children actually do when they use the Internet, though most parents control their children at least from time to time. Only 8 percent of parents use special programmes limiting children's access to unsuitable Internet pages. 51 percent of children aged 10 – 15 years has computer with internet in

	their children room. About 70 percent of the children aged 14-15 visits discussion groups on the internet 93 percent of children aged 10-11 let downloads and play online games More than a third of the children aged 14 – 15 years shares their personal data with unknown people on the internet 45 percent of the children aged 14 – 15 years shares their photographs and videos on the internet[141]
Indifference or reaction	None
Awareness campaigns/ results	Seznam.cz announced in June 2009 it produced an educational film for young users (12 – 16 years) on services Spoluzaci.cz and Lide.cz. Film is to present the risks of social networks especially related to misuse of networks by paedophiles. Company has also announced a plan to introduce from 2010 registration of the profiles through the SMS. According to product manager of social networks at Seznam.cz the measure is intended to limit a number of short term used profiles. "Up to 8 thousands of such profiles is created daily and part of them might be misused against children," said product manager Martin Kožíšek.[142] Seznam.cz also runs web pages Get acquinted safely[143] containing awareness materials on internet safety including films and Decalogue of internet safety, reporting button for internet abuse. However these pages contain very limited information on the way company itself deals with the data of the users. Several czech NGOs run awareness campaigns on the risks children face on the internet and offer also advices for safe behaviour and safety measures for both parents and children. Several web portals and help lines for referring of online abuse of a children were established. [144] Czech DPA created special web page advising principles and practical steps for securing childrens privacy online.[145] Special chapter in an online toolkit on protection of privacy in social networks was set up by NGO Iuridicum Remedium in May 2009.[146] During its European Presidency Czech government organised ministerial conference Safer Internet for Children where so called Pragues declaration was adopted.[147]
Good practises	See chapter Awareness campaigns

[141] *TNS AISA agency conducted its poll among pupils and students of basic and secondary schools and their parents in January 2009. The pollsters addressed 600 families and 319 of them returned the filled in questionnaires designed for children and especially for their parents to the pollsters, see http://www.ceskenoviny.cz/tema/index_view.php?id=378271&id_seznam=2058*

[142] *Dominik Hrodek: Seznam natočil výchovný film, in Strategie, 2009/06/01, p.10*

[143] *http://www.seznamsebezpecne.cz/*

[144] *see for instance: http://www.saferinternet.cz/, http://www.internethotline.cz/, http://www.internethelpline.cz/*

[145] *see http://www.uoou.cz/uoou.aspx?menu=287&submenu=335*

[146] *see http://www.uzijsisoukromi.cz/socialni-site/*

[147] *for Pragues declaration and presentations at the conference see http://www.mvcr.cz/mvcren/article/participants-of-the-conference-safer-internet-for-children-adopted-the-prague-declaration.aspx*

Campaign to be led. On which themes?	Awareness campaign on rights of the users of the social networks and implementation of better privacy protection practices by Seznam.cz, better informing on the way how company processes personal data.
Others	
Conclusions	
Recommendations	Agreement on social networking of the youth reached between European Commission and 17 companies operating social networks has show possibility of elevating of the levels of the privacy arrangements of the networks through public and political pressure. However measures introduced are still not satisfactory and they do not also apply to the adult users. Special focus need to be given to the practice of retaining of a data even from cancelled profiles and rules of transfer and procession of a data by a third parties (government bodies, other service providers, marketing and advertising companies). Companies providing service of social networks has also to adopt transparent information policy on the way they process or share data of the users.

43 - SPOLUZATI.CZ

Technology used/tool (For each teams, a card pro tool)	**Social network**
Country/ use area	Czech republic/
Frame of use	Spoluzaci.cz (means schoolmates.cz) free-access social networking website that is created and privately owned by Seznam.cz, a.s. Users can join networks organized by region, school, class. People can also chat, add friends and send them messages, and update their personal profiles to notify friends about themselves.
Population concerned: target and age	In February 2009 service spoluzaci.cz was most popular social network in the Czech republic used by 36 percent of the internet users.[148] According to the statistics of Seznam.cz and NetMonitor from April 2009 there were 228 719 real users daily[149] of which 7,30 percent of the users were 12 -14 years old, 20,53 percent 15 - 19 years old, 20,30 percent 20 – 25 years old.[150] According to the most recent figures, this social service attracted 206 083 real users daily in October 2009.[151]
% of users/of young users	See above
Trends (measured / supposed)	Slow growth of the numbers of the users in past half a year according to the data of the independent research project Net monitor.[152]
Known or potentials dangers /Risks	There were recently media reports on misuse of personal information submitted by the users for cyber bulling, black mailing of the girls.[153] According to the executive director of Seznam.cz Pavel Zima, company also sends to the Czech police every week two or three denouncements on possible paedophiles.[154] In 2008 media has reported that personal data of the elite czech

[148] *Facebook na místní servery stále nestačí,in ct24.cz of 2009/02/03, http://www.ct24.cz/media/44429-facebook-na-mistni-servery-stale-nestaci/*
[149] *see statistics of company Seznam.cz at http://onas.seznam.cz/cz/spoluzaci-cz.html*
[150] *statistics of Seznam.cz and NetMonitor, http://onas.szn.cz/onas/beta.onas.test/OUTPUT/Spoluzaci/spoluzaci_all_age.pdf*
[151] *see statistics of company Seznam.cz at http://onas.seznam.cz/cz/reklama/nase-internetove-servery/*
[152] *for detail see http://www.netmonitor.cz/*
[153] *Vladimír Rogl: ZNEUŽITÍ INTERNETU (Misuse of the Internet) in Slánské listy, 2009/04/28, p. 17,*
[154] *Dění na Internetu, in Lupa.cz of 2009/02/12, http://www.lupa.cz/clanky/seznam-v-roce-vnitrni-konsolidace/*
[155] *Jiří Reichl:Detektivové hazardují. Na webu odhalují soukromí, in Lidové noviny, 2008/03/21, http://www.lidovky.cz/detektivove-hazarduji-na-webu-odhaluji-soukromi-f6o-/ln_noviny.asp?c=A080321_000007_ln_noviny_sko&klic=224532&mes=080321_0*

[156] *45% zaměstnavatelů lustruje své potenciální zaměstnance přes sociální sítě in http://www.tyinternety.cz/socialni-site/45-zamestnavatelu-lustruje-sve-potencialni-zamestnance-pres-socialni-site-195 reffering to the report Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds, http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&cbsid=6e63b1d67ff8402bb65ce9ac927cab03-313226522-wt-6*

	undercovered detectives from organised crime unit including their telephone numbers, photographs and photographs of their children were posted by themselves on their personal profile at spoluzaci.cz. This report caused outrage at the Police presidium.[155] Despite the fact there has been recently some public discussions on the risks related to the misuse of posted data on the social networks for instance for profiling candidates for employment by companies)[156], many of the users are still ignoring possible risks.
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	Data submitted by the users and collected by Seznam.cz.[157]
What justifies the inscription in the file /Risks?	Consent of the user with Licence agreement of Seznam.cz/ However in this agreement it is not clearly defined how will be data further processed and stored. Company Seznam.cz there only states: «3) Everyone who filles any data on him/herself or other people in the framework of service Spoluzaci, gives this way his/her explicit consent according to § 5 of the No. 101/2000 Data protection act to the company Internet Pb, spol. s r.o., which is main contractor for the company Seznam.cz, a.s., and therefore processor of the data. These data will be publicised through the program placed at the server Spolužáci.cz, which means accessible to the unlimited number of people. This consent is given for unlimited time and can be anytime withdrawn by the form of covering letter adressed to the adress of Internet Pb, spol. s r.o. Company Internet Pb is covenant to delete without any delay all the personal information concerning respective person from the server Spolužáci.cz after delivery of the letter. Everyone who filles any data on him/herself or other people within the framework of server Spolužáci.cz, is aware the to the data submited can gain an access even a persons from other countries. Nobody is entitled, including company Internet Pb, spol. s r.o. to use the data for his/her profit. Companies Seznam.cz, a.s., and Internet Pb, spol. s r.o., are not responsible for accuracy of the data filled by third persons and accessible through the program placed at the server Spolužáci.cz nor for possible interference of third persons to these data. Internet Pb, spol. s r.o., is covenant not to collect, process, publicise and transfer personal data placed at the server Spolužáci.cz in the way that would contravene purpose ad nature of this program.»[158] / Wording of this Agreement obviously in some parts contravenes to each other and is the term of personal data and rights related to them is blured there.
Purposes /contents,	Purpose of the service is to offer a platform for electronic sharing of

[157] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*
[158] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*

main data included / Risks?	personal data and social contacts. It is also used for advertising and marketing purposes. / Data collected include: name, email address, telephone number, address, gender, schools attended, year of school education, and other personal (photographs, movies, messages) or preference information (links, friends links). Extend to which Seznam.cz also collects information on browser type and IP address of the user, certain information from browsers using 'cookies' is unclear./ for Risks see Known or potentials dangers
File masters? Risks?	Data submitted by users, processor of the data is company Seznam.cz
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Access to the file is restricted by simple login, part to the data (name, surname, respective school and year of finishing of studies) available to everyone, other just to approved «friends»
Data retention delays/ risks Right to be forgotten	Unclear – according to the Licence agreement of Seznam.cz user can cansel his/her account it is unclaer however from the agreement what will happen with collected data. Wording of the Licence agreement also provides for censorship of improper content by the operator.[159]
Rights to know or to modify data?	See Data retention delays/ risks/ Right to be forgotten
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	None specific national legislation adopted, EU DP directives applies however there is lack of enforcement of those directives in the case of social networks.
Risks for freedoms despite the law	Data included in social network database can be misused for profiling, collecting of personal informations by third parties, discrimination etc.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen

[159] *Licence agreement of Seznam.cz, http://registrace.seznam.cz/register.py/stageZeroScreen?service=email*

Conformity with the European right (Charter of fundamental rights, directives…)	Procession of the data probably not meeting european standards set by: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001.
Implementation (or not) of the legislation? / Risks	There was not any result of investigation into conformity of the practice of social networks with DP legislation published by the DPA, nor position of DPA issued on this matter.
Others	
This tools and young public or young adults	
How far are young people concerned?	See % of users/of young users
Awareness of issues or of risks	More general research on awareness of the children about the risks on the internet and behaviour of the children related to internet was publicised in May 2009. From the results: Czech children on average spend on the Internet 12 hours a week. More than one-third of children aged 14-15 provide unknown people with their personal and contact data through the Internet. 17 percent of parents pay no interest to what their children actually do when they use the Internet, though most parents control their children at least from time to time. Only 8 percent of parents use special programmes limiting children's access to unsuitable Internet pages. 51 percent of children aged 10 – 15 years has computer with internet in their children room. About 70 percent of the children aged 14-15 visits discussion groups on the internet 93 percent of children aged 10-11 let downloads and play online games More than a third of the children aged 14 – 15 years shares their personal data with unknown people on the internet 45 percent of the children aged 14 – 15 years shares their photographs and videos on the internet[160]
Indifference or reaction	None

[160] *TNS AISA agency conducted its poll among pupils and students of basic and secondary schools and their parents in January 2009. The pollsters addressed 600 families and 319 of them returned the filled in questionnaires designed for children and especially for their parents to the pollsters, see http://www.ceskenoviny.cz/tema/index_view.php?id=378271&id_seznam=2058*

Awareness campaigns/ results	Seznam.cz announced in June 2009 it produced an educational film for young users (12 – 16 years) on services Spoluzaci.cz and Lide.cz. Film is to present the risks of social networks especially related to misuse of networks by paedophiles. Company has also announced a plan to introduce from 2010 registration of the profiles through the SMS. According to product manager of social networks at Seznam.cz the measure is intended to limit a number of short term used profiles. "Up to 8 thousands of such profiles is created daily and part of them might be misused against children," said product manager Martin Kožíšek.[161] Seznam.cz also runs web pages Get acquinted safely[162] containing awareness materials on internet safety including films and Decalogue of internet safety, reporting button for internet abuse. However these pages contain very limited information on the way company itself deals with the data of the users. Several czech NGOs run awareness campaigns on the risks children face on the internet and offer also advices for safe behaviour and safety measures for both parents and children. Several web portals and help lines for referring of online abuse of a children were established. [163] Czech DPA created special web page advising principles and practical steps for securing childrens privacy online.[164] Special chapter in an online toolkit on protection of privacy in social networks was set up by NGO Iuridicum Remedium in May 2009.[165] During its European Presidency Czech government organised ministerial conference Safer Internet for Children where so called Pragues declaration was adopted.[166]
Good practises	See chapter Awareness campaigns
Campaign to be led. On which themes?	Awareness campaign on rights of the users of the social networks and implementation of better privacy protection practices by Seznam.cz, better informing on the way how company processes personal data.
Others	
Conclusions	
Recommendations	Agreement on social networking of the youth reached between European Commission and 17 companies operating social networks has show possibility of elevating of the levels of the privacy arrangements of the networks through public and political pressure. However measures introduced are still not satisfactory and they do not also apply to the adult users. Special focus need to be given to the practice of retaining of a data even from cancelled profiles and rules of transfer and procession of a data by a third parties (government bodies, other service providers, marketing and advertising companies). Companies providing service of social networks has also to adopt transparent information policy on the way they process or share data of the users.

[161] *Dominik Hrodek: Seznam natočil výchovný film, in Strategie, 2009/06/01, p.10*
[162] *http://www.seznamsebezpecne.cz/*
[163] *see for instance: http://www.saferinternet.cz/, http://www.internethotline.cz/, http://www.internethelpline.cz/*
[164] *see http://www.uoou.cz/uoou.aspx?menu=287&submenu=335*
[165] *see http://www.uzijsisoukromi.cz/socialni-site/*
[166] *for Pragues declaration and presentations at the conference see http://www.mvcr.cz/mvcren/article/participants-of-the-conference-safer-internet-for-children-adopted-the-prague-declaration.aspx*

44 – FACEBOOK

Country/ use area	Czech republic/ Worldwide
Frame of use	free-access social networking website that is operated and privately owned by Facebook, Inc. Users can join networks organized by city, workplace, school, and region to connect and interact with other people. People can also add friends and send them messages, and update their personal profiles to notify friends about themselves.[167]
Population concerned: target and age	According to the statistics of Facebook there were 200000 registered users older than 15 years from the Czech republic at the beginning of 2009. 54 percent of them were women, 44 percent of the Czech users of Facebook were between 21 and 25 years of age.[168] Latest figures revealed 1667960 of the Czech users of the Facebook among whom approx. 20 percent are of 14 to 17 years of age, 36,4 percent of 18 to 24 years of age.[169]
% of users/of young users	See above
Trends (measured / supposed)	Rapidly growing numbers of users in a past three years according to the data of the independent research project Net monitor.[170]
Known or potentials dangers /Risks	Several concerns have emerged regarding the use of Facebook as a means of surveillance and data mining. Two MIT students were able to download over 70,000 Facebook profiles from four schools (MIT, New York University, the University of Oklahoma, and Harvard University) using an automated shell script, as part of a research project on Facebook privacy published on December 14, 2005. The possibility of data mining remains open, as evidenced in May 2008, when the BBC technology program „Click“ demonstrated that personal details of Facebook users and their friends could be stolen by submitting malicious applications. Privacy proponents have criticized the site's privacy agreement, which states: "We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile."Another clause that received criticism concerned Facebook's right to sell a user's data to private companies, stating: "We may share your information with third parties, including responsible companies with which we have a relationship." This concern was addressed by Facebook spokesman Chris Hudges who said, "Simply put, we have never provided our users' information to third party companies, nor do we intend to. Concerns have also been raised regarding the difficulty of deleting user accounts. Previously, Facebook only allowed users to "deactivate" their accounts so that their profile was no longer visible. However, any information

[167] *see http://en.wikipedia.org/wiki/Facebook*
[168] *Ješátko Vojtěch, Komunitní marketing in Marketing Journal, no. 1/09, publicised 2009/02/18, http://www.m-journal.cz/cs/marketing/nove-trendy/komunitni-marketing__s302x5052.html*
[169] *for details see statistics of Facebook at CheckFacebook.com*
[170] *for detail see http://www.netmonitor.cz/*

	the user had entered into the website and on their profile remained on the website's servers. This outraged many users who wished to remove their accounts permanently, citing reasons such as the inability to erase "embarrassing or overly-personal online profiles from their student days as they entered the job market, for fear employers would locate the profiles" Facebook changed its account deletion policies on February 29, 2008, allowing users to contact the website to request that their accounts be permanently deleted. On May 7, 2009 it was revealed by the New York Times that a bug allowed personal e-mail addresses of Facebook users to be easily accessible. The bug was fixed "within hours of it being reported to us".[171] Despite the fact there has been recently some public discussions on the risks related to the misuse of posted data on the social networks for instance for profiling candidates for employment by companies)[172], many of the users are still ignoring possible risks.
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	Data submitted by the users and collected by the Facebook during the use of the service are processed in Facebook databases.[173]
What justifies the inscription in the file /Risks?	Consent of the users with Statement of Rights and Responsibilities of Facebook service[174]
Purposes /contents, main data included / Risks?	Purpose of the service is to offer a platform for electronic sharing of personal data and social contacts. It is also used for advertising and marketing purposes. / Data collected include: name, email address, telephone number, address, gender, schools attended and other personal (photographs, movies, messages) or preference information (links, friends links). Facebook also collects information on browser type and IP address of the user, certain information from browsers using 'cookies'.[175]/ for Risks see Known or potentials dangers
File masters? Risks?	Facebook and other service providers
Who accesses the files/ Sharing of the data base? Access limits? /Risks	User can limit accesibility of some of his/her personal information to the friends on the list. Personal information are accessed by Facebook, other service providers and law enforcement agencies of the US.[176]
Data retention delays/	Unclear – Facebook privacy principles says: „Access and control over most personal information on Facebook is readily available through the Profile

[171] *see http://en.wikipedia.org/wiki/Facebook#Privacy*

172 45% zaměstnavatelů lustruje své potenciální zaměstnance přes sociální sítě in http://www.tyinternety.cz/socialni-site/45-zamestnavatelu-lustruje-sve-potencialni-zamestnance-pres-socialni-site-195 reffering to the report Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds, http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&cbsid=6e63b1d67ff8402bb65ce9ac927cab03-313226522-wt-6

[173] *for details see http://www.facebook.com/policy.php?ref=pf*
[174] *for details see http://www.facebook.com/policy.php?ref=pf#/terms.php*
[175] *for details see http://www.facebook.com/policy.php?ref=pf*
[176] *for details see http://www.facebook.com/policy.php?ref=pf*

risks Right to be forgotten	editing tools. Facebook users may modify or delete any of their Profile information at any time by logging into their account. Information will be updated immediately. Individuals who wish to deactivate their Facebook account may do so on the My Account page. Removed information may persist in back-up copies for a reasonable period of time but will not be generally available to members of Facebook. Where you make use of the communication features of the service to share information with other individuals on Facebook, however, (e.g. sending a personal message to another Facebook user) you generally cannot remove such communications."[177]
Rights to know or to modify data?	See Data retention delays/ risks/ Right to be forgotten
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	None specific national legislation adopted, EU DP directives applies however there is lack of enforcement of those directives in the case of social networks.
Risks for freedoms despite the law	Data included in social network database can be misused for profiling, collecting of personal informations by third parties, discrimination etc.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Procession of the data probably not meeting european standarts set by: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001.
Implementation (or not) of the legislation? / Risks	There was not any result of investigation into conformity of the practice of social networks with DP legislation published by the DPA, nor position of DPA issued on this matter.

[177] *see http://www.facebook.com/home.php#/policy.php?ref=pf*

Others	
This tools and young public or young adults	
How far are young people concerned?	See % of users/of young users
Awareness of issues or of risks	More general research on awareness of the children about the risks on the internet and behaviour of the children related to internet was publicised in May 2009. From the results: Czech children on average spend on the Internet 12 hours a week. More than one-third of children aged 14-15 provide unknown people with their personal and contact data through the Internet. 17 percent of parents pay no interest to what their children actually do when they use the Internet, though most parents control their children at least from time to time. Only 8 percent of parents use special programmes limiting children's access to unsuitable Internet pages. 51 percent of children aged 10 – 15 years has computer with internet in their children room. About 70 percent of the children aged 14-15 visits discussion groups on the internet 93 percent of children aged 10-11 let downloads and play online games More than a third of the children aged 14 – 15 years shares their personal data with unknown people on the internet 45 percent of the children aged 14 – 15 years shares their photographs and videos on the internet[178]
Indifference or reaction	None
Awareness campaigns/ results	Several czech NGOs run awareness campaigns on the risks children face on the internet and offer also advices for safe behaviour and safety measures for both parents and children. Several web portals and help lines for referring of online abuse of a children were established. [179] Czech DPA created special web page advising principles and practical steps for securing childrens privacy online.[180] Special chapter in an online toolkit on protection of privacy in social networks was set up by NGO Iuridicum Remedium in May 2009.[181]

[178] *TNS AISA agency conducted its poll among pupils and students of basic and secondary schools and their parents in January 2009. The pollsters addressed 600 families and 319 of them returned the filled in questionnaires designed for children and especially for their parents to the pollsters, see http://www.ceskenoviny.cz/tema/index_view.php?id=378271&id_seznam=2058*

[179] *see for instance: http://www.saferinternet.cz/, http://www.internethotline.cz/, http://www.internethelpline.cz/*
[180] *see http://www.uoou.cz/uoou.aspx?menu=287&submenu=335*
[181] *see http://www.uzijsisoukromi.cz/socialni-site/*

	During its European Presidency Czech government organised ministerial conference Safer Internet for Children where so called Pragues declaration was adopted.[182]
Good practises	Facebook was among 17 companies that has signed agreement on social networking rules for youth under 18 in February 2009. Rules aimed at reducing of the privacy and security risks related to the usage of social networks include: Providing an easy to use and accessible "report abuse" button, allowing users to report inappropriate contact from or conduct by another user with one click. Making sure that the full online profiles and contact lists of website users who are registered as under 18s are set to "private" by default. This will make it harder for people with bad intentions to get in touch with the young person. Ensuring that private profiles of users under the age of 18 are not searchable (on the websites or via search engines) Guaranteeing that privacy options are prominent and accessible at all times, so that users can easily work out if just their friends, or the entire world, can see what they post online. Preventing under-age users from using their services: if a social networking site targets teenagers over 13, it should be difficult for people below that age to register.[183]
Campaign to be led. On which themes?	Awareness campaign on rights of the users of the social networks and implementation of better privacy protection practices by Facebook.
Others	
Conclusions	
Recommendations	Agreement on social networking of the youth reached between European Commission and 17 companies operating social networks has show possibility of elevating of the levels of the privacy arrangements of the networks through public and political pressure. However measures introduced are still not satisfactory and they do not also apply to the adult users. Special focus need to be given to the practice of retaining of a data even from cancelled profiles and rules of transfer and procession of a data by a third parties (government bodies, other service providers, marketing and advertising companies).

[182] *for Pragues declaration and presentations at the conference see http://www.mvcr.cz/mvcren/article/participants-of-the-conference-safer-internet-for-children-adopted-the-prague-declaration.aspx*

[183] *Social Networking: Commission brokers agreement among major web companies, 2009/02/10, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232*

5 - AUTRES

51 - CENTRALISED DATABASE OF INFORMATION FROM SCHOOL REGISTERS

Country/ use area	Czech republic/ Prague
Frame of use	Registers were established for statistical, analytical and budgetary purposes of state educational policy[184] and economical and organisational purposes of the individual school institutions. The files on individual students are created by school administration in individual schools and than submitted to the regional government which passes the information to the Ministry of education. Some schools also submit data directly to Ministry of education[185] which passes the data o special state research and statistical institution - Institute for Information on Education.[186]
Population concerned: target and age	Pupils, students of primary, secondary and high schools
% of users/of young users	Overwhelming majority of a data subjects are youngsters under 26 years of age[187]
Trends (measured / supposed)	Growing numbers of a subjects of a data included in database. Process started in 2005/06 by collecting data from high schools, in 2006/07 data on students of secondary schools and art schools were included, in 2008/09 data on pupils and students of most of the schools offering primary, secondary and high school education were included in the system.[188] By the May 2009 data on approx. 800 thousand students and pupils were included, in a future number is expected to be doubled.[189]
Known or potentials dangers /Risks	Suspected leakages of a data from registers to a commercial subjects led DPA to start investigation.[190]
Others	
Generated data bases	

[184] Education Act No. 561/2004 On Pre-primary, Basic, Secondary and Tertiary Professional Education

[185] *Education Act No. 561/2004 On Pre-primary, Basic, Secondary and Tertiary Professional Education, Ordinances no 364/2005., no. 389/2006 and no. 226/2007 of the Ministry of education*

[186] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*

[187] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*

[188] *Information on transfer of a data from the school registers of primary, secondary, high schools and art schools for central processing, http://skoly.praha-mesto.cz/78409_Informace-k-predavani-udaju-ze-skolnich-matrik-ZS-SS-VOS-a-konzervatori-k-centralnimu-zpracovani*

[189] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*

[190] *Vladimír Křivka - Fond ohrožených dětí čelí trestnímu oznámení, in Týden weekly 2009/1/8*

Associated data base/ creation (a line pro database)	Data from registers of pupils and students of individual schools are twice a year submitted in the electronical form to the central database of the Ministry of education.
What justifies the inscription in the file /Risks?	Statistical, analytical and budgetary purposes of state educational policy and economical purposes of schools. The state subsidy to the school institution is set according to the actual number of pupils in fields and forms of education put in the school register[191]
Purposes /contents, main data included / Risks?	Following data are processed in central database : birth number, year and month of birth, nationality, code of adress, information on previous education, information on actual year, type, form and specialisation of the class attended, foreign languages, information on interruptions of education or repetitions of classes, information on type of finished exams and numbers of certificates of reached education levels.[192]
File masters? Risks?	Ministry of education – processor. Data on subjects are filled into the system by the administrators at individual schools.[193]
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Authorised access of limited number of administrators and analytics. Access to the files is audited and each user needs special login.[194]
Data retention delays/ risks Right to be forgotten	Unclear/according to information of Institute for Information on Education are data after finishing of education of the subject kept in anonymised form[195]
Rights to know or to modify data?	Subjects (their parents) can ask processor of their data at their individual school register to correct the data.[196] They are not asked to give their consent with the procession of their data according to the Institute for Information on Education parents are also informed by the school administration of the way data of their children are further processed, shared and how they can modify them. However detail information on the way data are processed is not so far publicly available.
Covert purposes/ Risks/uncontrolled future evolution	Risks evolving from unclear system of administration of users rights, possible extention of the rights to share files on other subjects (state administration, private companies providing services to the ministry?)

[191] Jana Kohoutková: UNION STUDENTS' REGISTER:Data Integration to Support National Education Management, presentation of 2000/4/14
www.man.poznan.pl/ist/eunis/programme/EUNIS2000/slides/kohoutkova/eunis-kohoutkova.PPT
[192] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*
[193] *FaQs at Institute for Information on Education web pages http://www.uiv.cz/clanek/525/1181*
[194] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*
[195] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*
[196] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*

Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Education Act No. 561/2004 On Pre-primary, Basic, Secondary and Tertiary Professional Education, Ordinances no 364/2005., no. 389/2006 and no. 226/2007 of the Ministry of education
Risks for freedoms despite the law	Subjects are not informed of the extend and ways of the processing of their data nor their related rights. Discrimination in access to the education or social benefits related to the mistaken data or faults in databases may occur.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Probably not conforming with Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001.
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	See % of users/of young users
Awareness of issues or of risks	None research made so far, probably very low
Indifference or reaction	None
Awareness campaigns/ results	None
Good practises	Auditing of the access to the files

Campaign to be led. On which themes?	Awareness campaign on extend of data currently processed, importance of free consent with data protection and legislation change
Others	
Conclusions	
Recommendations	Clarification of a concept of the registers. Inclusion of free consent of the students with the procession of the data. Replacing the system of identification of the students by their birth number with source identification number. Clear and strict measures on right to access the data. Information campaign on purposes and practice of operation of central database.

52 - DATABASE OF UNION INFORMATION FROM STUDENTS' REGISTERS

Identification of technology	**Database of Union *Information* from *Students' Registers* - Sdružené informace matrik studentů (SIMS)**
Technology used/tool (For each teams, a card pro tool)	**Database of university students**
Country/ use area	Czech republic/ Prague
Frame of use	Registers were established for statistical, analytical and budgetary purposes of state educational policy[197] and economical and organisational purposes of universities.[198] They are used by individual faculties, universities, Ministry of Education, Institute for Information on Education (statistical purposes)
Population concerned: target and age	University students and former university students
% of users/of young users	More than 67 percent of youngsters up to 26 years of age[199]
Trends (measured / supposed)	Growing numbers of a subjects of a data included in database – 801 103 subjects of a data in May 2009[200], approx. 0,5 million subjects of a data in 2006[201]
Known or potentials dangers /Risks	Suspected leakages of a data from registers to a commercial subjects led DPA to start investigation.[202]
Others	
Generated data bases	
Associated data base/ creation (a line pro database)	Data from registers of students of individual faculties, universities are four times a year submitted to the Database of Union Information from Students´Register/ Registers started to be created from 1998 when a new

[197] *Act no. 111/1998 Sb., on universities, § 87, art. i)*

[198] *Act no. 111/1998 Sb., on universities, § 88*

[199] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*

[200] *from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21*

[201] *Ing. Mgr. Jiří Šmerda : Union Students Register (SIMS) (student thesis), http://is.muni.cz/th/60444/fi_m/thesis-xsmerda2.pdf*

[202] *Vladimír Křivka - Fond ohrožených dětí čelí trestnímu oznámení, in Týden weekly 2009/1/8*

	law on universities was approved. The law provided that every university has to establish a register of students with detailed set of a data. Public bid for technical solution of the united general register won Institute of Computer Science of Maysaryk University that mantains operates the register for Ministry of Education until today.[203]
What justifies the inscription in the file /Risks?	Statistical, analytical and budgetary purposes of state educational policy and economical purposes of universities
Purposes /contents, main data included / Risks?	records (extended) about all CZ university students & their studies (incl. histories: birthcode,name, surname, domicile region, state, previous education, uni/faculty, programme, study start, programme type, study length, newly admitted, dormitory, study end (date, form),study Histories, state code/citizenship, edu location, study form, study break, form of financing, parallel studies, total study length, financing (verif), budgetary student includes data since 01/01/1999[204]
File masters? Risks?	Ministry of education – processor. Operated by Institute of Computer Science of Maysaryk University. Three different types of users: - administrator – can edit and see any data - user from the university – can edit and see only some data - user from the ministry of education (Institute) - unclear Administration and creation of user accounts is not providing an easy survey. There were plans to centralise and clarify and standardise decisions on rights of the users – it is not clear however if they were implemented.[205]
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Ministry passes login and password on access to the SIMS on legal representative of the university. processor of register of individual faculty has the rights to access central databasis SIMS and edit and create there files and other users accounts.[206] Files are furthermore accessed by single responsible person at Institute for Information on Education. who is later on anonymising them for statistical purposes.[207]
Data retention delays/ risks Right to be forgotten	Unclear/according to information of Institute for Information on Education are data after finishing of education of the subject kept in anonymised form
Rights to know or to	Subjects can ask processor of their data at their individual faculty register to

[203] Ing. Mgr. Jiří Šmerda : Union Students Register (SIMS) (student thesis), http://is.muni.cz/th/60444/fi_m/thesis-xsmerda2.pdf, from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21
[204] Jana Kohoutková: UNION STUDENTS' REGISTER:Data Integration to Support National Education Management, presentation of 2000/4/14 ww*w.man.poznan.pl/ist/eunis/programme/EUNIS2000/slides/kohoutkova/eunis-kohoutkova.PPT*
[205] Ing. Mgr. Jiří Šmerda : Union Students Register (SIMS) (student thesis), http://is.muni.cz/th/60444/fi_m/thesis-xsmerda2.pdf
[206] Login into system SIMS, http://sims.ics.muni.cz/
[207] from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21
[208] from the response of the Institute for Information on Education (**Ústav pro informace ve vzdělávání**) to the request of Iuridicum Remedium of 2009/5/21

modify data?	correct the data.[208] They are not asked to give their consent with the procession of their data nor they are informed of the way their data are further processed, shared and how they can modify them.
Covert purposes/ Risks/uncontrolled future evolution	Risks evolving from unclear system of administration of users rights, possible extention of the rights to share files on other subjects (state administration, private companies providing services to faculties of ministry)
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Act no. *111/1998 Sb*., on universities,
Risks for freedoms despite the law	Subjects are not informed of the extend of the processing of their data nor their related rights. Discrimination in access to the education or social benefits related to the mistaken data or faults in databases may occur.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Not foreseen
Conformity with the European right (Charter of fundamental rights, directives…)	Probably not conforming with Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108), The Czech Republic ratified the Convention CETS No. 108 on 9 July 2001 and it entered into force in the Czech Republic on 1 November 2001.
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	See % of users/of young users
Awareness of issues or of risks	None research made so far, probably very low
Indifference or reaction	None

Awareness campaigns/ results	None
Good practises	None
Campaign to be led. On which themes?	Awareness campaign on extend of data currently processed, importance of free consent with data protection and legislation change
Others	
Conclusions	
Recommendations	Clarification of a concept of the registers. Inclusion of free consent of the students with the procession of the data. Replacing the system of identification of the students by their birth number with source identifier. Clear and strict measures on right to access and edit the data, auditing of access to the data.