

# IURIDICUM REMEDIUM

Iuridicum Remedium, o.s se sídlem Vírská 14/278, 198 00 Praha 9, IČO: 265 34 487

Kancelář: U Průhonu 23/1201, 170 00 Praha 7, tel/fax: +420 222 515 564

e-mail: iure@iure.cz, web: <http://www.iure.org>

<http://www.slidilove.cz>

## Table of contents

### Identical frame for each country

#### *Introduction and methodological choices*

#### **1 Mobility and transportation**

##### **1 – Inventory of technologies**

Methodology used for the inventory of technologies and details about the field investigated  
Analysis of data (inventory of technologies) in order to identify which are most used and which are used especially by young people.

Outlines of trends for the relative importance of the various technologies, scale of use.

Technologies selected for a thorough work (detailed cards): reasons of the choice and interest for our study

Synthesis on the selected technologies for the detailed cards: known or potential dangers, importance of the use, trends (development, regression),.

##### **2 – Data bases generated and their objects, risks induced**

Synthesis gathering information of the cards carried out and trends (see card standard page 5-6)

Is the use in conformity with the European recommendations?

Trends proven (or not) for a drift or a diversion of the use of the files towards survey, commercial use...

##### **3 – The legislation which frames the use of technologies and the generated data bases, their limits regarding freedoms**

Synthesis: characteristics of the legislation

Conformity with the European recommendations or with the European right

Analysis: acknowledged purposes and potential drifts of use

Implementation (or not) of the legislation

Analysis: is the legislation protective enough? Needs to re-examine the legislation? Why?

##### **4 – These tools and young people and young adults: awareness of risks**

Synthesis of the data with

- On which scale the young people and young adults are concerned, trends

- Awareness of dangers, attitude of young people and young adults with respect to these risks, concerns to have

- Existing public awareness campaigns; evaluation of these campaigns and their impact: good practices, is it necessary to do more, fields of necessary interventions

##### **5 – Conclusions: which evolutions for legislation and awareness tools**

Necessary evolutions in the legislative framing

Evolutions/ necessary campaigns for young people to become aware of risks and dangers

Recommendations

## **2 Biological identity**

### **1 – Inventory of technologies**

Methodology used for the inventory of technologies and details about the field investigated  
Analysis of data (inventory of technologies) in order to identify which are most used and which are used especially by young people.

Outlines of trends for the relative importance of the various technologies, scale of use.

Technologies selected for a thorough work (detailed cards): reasons of the choice and interest for our study

Synthesis on the selected technologies for the detailed cards: known or potential dangers, importance of the use, trends (development, regression),.

### **2 – Data bases generated and their objects, risks induced**

Synthesis gathering information of the cards carried out and trends (see card standard page 5-6)

Is the use in conformity with the European recommendations?

Trends proven (or not) for a drift or a diversion of the use of the files towards survey, commercial use...

### **3 – The legislation which frames the use of technologies and the generated data bases, their limits regarding freedoms**

Synthesis: characteristics of the legislation

Conformity with the European recommendations or with the European right

Analysis: acknowledged purposes and potential drifts of use

Implementation (or not) of the legislation

Analysis: is the legislation protective enough? Needs to re-examine the legislation? Why?

### **4 – These tools and young people and young adults: awareness of risks**

Synthesis of the data with

- On which scale the young people and young adults are concerned, trends
- Awareness of dangers, attitude of young people and young adults with respect to these risks, concerns to have
- Existing public awareness campaigns; evaluation of these campaigns and their impact: good practices, is it necessary to do more, fields of necessary interventions

### **5 – Conclusions: which evolutions for legislation and awareness tools**

Necessary evolutions in the legislative framing

Evolutions/ necessary campaigns for young people to become aware of risks and dangers

Recommendations

## **3 Interpersonal communications**

### **1 – Inventory of technologies**

Methodology used for the inventory of technologies and details about the field investigated

Analysis of data (inventory of technologies) in order to identify which are most used and which are used especially by young people.

Outlines of trends for the relative importance of the various technologies, scale of use.

Technologies selected for a thorough work (detailed cards): reasons of the choice and interest for our study

Synthesis on the selected technologies for the detailed cards: known or potential dangers, importance of the use, trends (development, regression),.

### **2 – Data bases generated and their objects, risks induced**

Synthesis gathering information of the cards carried out and trends (see card standard page 5-6)

Is the use in conformity with the European recommendations?

Trends proven (or not) for a drift or a diversion of the use of the files towards survey, commercial use...

### **3 – The legislation which frames the use of technologies and the generated data bases, their limits regarding freedoms**

Synthesis: characteristics of the legislation

Conformity with the European recommendations or with the European right

Analysis: acknowledged purposes and potential drifts of use

Implementation (or not) of the legislation

Analysis: is the legislation protective enough? Needs to re-examine the legislation? Why?

#### **4 – These tools and young people and young adults: awareness of risks**

Synthesis of the data with

- On which scale the young people and young adults are concerned, trends
- Awareness of dangers, attitude of young people and young adults with respect to these risks, concerns to have
- Existing public awareness campaigns; evaluation of these campaigns and their impact: good practices, is it necessary to do more, fields of necessary interventions

#### **5 – Conclusions: which evolutions for legislation and awareness tools**

Necessary evolutions in the legislative framing

Evolutions/ necessary campaigns for young people to become aware of risks and dangers

Recommendations

### ***4 Social networks and new gate keepers of communications***

#### **1 – Inventory of technologies**

Methodology used for the inventory of technologies and details about the field investigated

Analysis of data (inventory of technologies) in order to identify which are most used and which are used especially by young people.

Outlines of trends for the relative importance of the various technologies, scale of use.

Technologies selected for a thorough work (detailed cards): reasons of the choice and interest for our study

Synthesis on the selected technologies for the detailed cards: known or potential dangers, importance of the use, trends (development, regression),.

#### **2 – Data bases generated and their objects, risks induced**

Synthesis gathering information of the cards carried out and trends (see card standard page 5-6)

Is the use in conformity with the European recommendations?

Trends proven (or not) for a drift or a diversion of the use of the files towards survey, commercial use...

#### **3 – The legislation which frames the use of technologies and the generated data bases, their limits regarding freedoms**

Synthesis: characteristics of the legislation

Conformity with the European recommendations or with the European right

Analysis: acknowledged purposes and potential drifts of use

Implementation (or not) of the legislation

Analysis: is the legislation protective enough? Needs to re-examine the legislation? Why?

#### **4 – These tools and young people and young adults: awareness of risks**

Synthesis of the data with

- On which scale the young people and young adults are concerned, trends
- Awareness of dangers, attitude of young people and young adults with respect to these risks, concerns to have
- Existing public awareness campaigns; evaluation of these campaigns and their impact: good practices, is it necessary to do more, fields of necessary interventions

#### **5 – Conclusions: which evolutions for legislation and awareness tools**

Necessary evolutions in the legislative framing

Evolutions/ necessary campaigns for young people to become aware of risks and dangers

Recommendations

## ***Conclusions***

## **For each chapter, we propose**

- **that the researches will give a report as exhaustive as possible on technologies, tools, supports used**
- **that a choice will be made on technologies, tools,... which are most interesting to analyze. They will be detailed in a “card” (our proposal hereafter)**
- **that by chapter (4 chapters) we will have an average of some ten card detailed for France, the Czech Republic and Spain while EDRI and the AEDH will limit this exercise at 3 cards detailed by chapter (4 chapters) for each country. This is given as an indication: of course it is necessary to modulate according to the chapters and to the interest that each card brings. It can be more relevant to deepen a card rather than to multiply the number of cards: each partner will estimate this relevance.**
- **these cards will be attached to each chapter which will present in approximately 5/7 pages per chapter a synthesis (about 25 pages of analysis and synthesis accompanied by 40 detailed cards or a dozen cards for each country “AEDH” or “EDRI”). Here still the lengths are given as an indication.**
- **It should be stressed that each chapter presents at the same time synthetic aspects and analytical aspects, based on the cards carried out and the accumulated knowledge.**

## Frame of the cards: identical structure for each country

<b>THEME</b>	<b>MOBILITY</b>	
<b>Identification of technology</b>	<b>Pragues opencard</b>	
<b>Technology used/tool</b> (For each teams, a card pro tool)	<b>RFID CARD/ smart – card</b>	
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 <sup>1</sup> after RFID card was made obligatory for anyone seeking annual discount card for 2009.	
Known or potentials dangers /Risks	<p>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.<sup>2</sup></p> <p>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.<sup>3</sup></p> <p>Information on unique ID of the RFID chips gathered from inspectors and</p>	

<sup>1</sup> press release of the project opencard  
[http://opencard.praha.eu/jnp/cz/aktuality/pro\\_media/podminky\\_pro\\_nahravani\\_kuponu\\_pid\\_na.html](http://opencard.praha.eu/jnp/cz/aktuality/pro_media/podminky_pro_nahravani_kuponu_pid_na.html)

<sup>2</sup> press release of NGO Iuridicum Remedium of 29.7.2007  
<http://zpravodajstvi.ecn.cz/index.stm?x=2020676>

<sup>3</sup> Chris Johnstone, Prague transport company seeks to bring back metro turnstiles, 18.3.2009 in <http://www.radio.cz/en/article/114326>

	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 and other certified data of the providers of the services.	
<b>Generated data bases</b>		
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, authentication 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) <sup>4</sup> , 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 contact 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 generally needed so inspectors can recognise authorised user of the card. Data protection office argues however : <i>«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»<sup>5</sup></i>	
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 furthermore empower private «processors» to process and store collected data: HAGUESS, a.s., (ID	

<sup>4</sup> conditions of the contract – opencard

[http://opencard.praha.eu/jnp/cz/podminky/zpracovani\\_osobnich\\_udaju.html](http://opencard.praha.eu/jnp/cz/podminky/zpracovani_osobnich_udaju.html)

<sup>5</sup> Czech Data protection authority Annual Report 2008

	of organisation 250 85 166), Assecó Czech Republic, a.s.. (27074358), Monet+, a.s., (262 17 783), STATNÍ 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) <sup>6</sup>	
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 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. <sup>7</sup>	
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 authority 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	

<sup>6</sup> conditions of the contract – opencard

[http://opencard.praha.eu/jnp/cz/podminky/zpracovani\\_osobnich\\_udaju.html](http://opencard.praha.eu/jnp/cz/podminky/zpracovani_osobnich_udaju.html)

<sup>7</sup> conditions of the contract – opencard

[http://opencard.praha.eu/jnp/cz/podminky/zpracovani\\_osobnich\\_udaju.html](http://opencard.praha.eu/jnp/cz/podminky/zpracovani_osobnich_udaju.html)

	<p>habits, reading preferences, 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.</p>	
Others (interconnections...)	<p>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.</p>	
<b>Legislation in application</b>		
<p>Law /rules / others (?) (implemented for this data base or this technology)</p>	<p>No specific legislation on RFID use</p> <p>Personal Data Protection Act, Act 101 of April 4, 2000</p> <p>Chapter II</p> <p>Rights and obligations in processing of personal data</p> <p>Article 5</p> <p>(1) The controller shall be obliged to:</p> <p>(a) specify the purpose for which personal data are to be processed;</p> <p>(b) specify the means and manner of personal data processing;</p> <p>(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</p>	

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

	<p>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.</p> <p>Article 7</p> <p>The obligations specified in Article 5 shall apply to the processor mutatis mutandis.</p> <p>Article 8</p> <p>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.</p>	
<p>Risks for freedoms despite the law</p>	<p>Complex technical and organisational solution makes very difficult to assess 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 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.</p>	
<p>If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)</p>	<p>Not foreseen</p>	
<p>Conformity with the European right (Charter of fundamental rights, directives...)</p>	<p>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.</p> <p>Article 5 – Quality of data</p> <p>Personal data undergoing automatic</p>	

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		
<b>This tools and young public or young adults</b>		
How far are young people concerned?	Create significant part of the users, number not revealed	
Awareness of issues or of risks	Partial	
Indifference or reaction	800 signatures under the petition for introduction of anonymous smart-card	
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		
<b>Conclusions</b>	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.  Establishing a new legislation specifically focused on RFID.	

Podpořili nás:



Ministerstvo práce a sociálních věcí

Trust for Civil Society in Central & Eastern Europe

Open Society Fund Praha



OPERAČNÍ PROGRAM  
LIDSKÉ ZDROJE  
A ZAMĚSTNANOST

PODPORUJEME  
VAŠI BUDOUCNOST  
[www.esfcr.cz](http://www.esfcr.cz)



nadace rozvoje  
občanské společnosti



Podpořeno grantem z Islandu, Lichtenštejska a Norska v rámci

Finančního mechanismu EHP a Norského finančního mechanismu

prostřednictvím Nadace rozvoje občanské společnosti.