



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

Frame of the cards: identical structure for each country

THEME	MOBILITY	
Identification of technology	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 <i>loyalty card</i> 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, ¹ in April 2009 In-Karta was used by 400000 customers. ²	
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. ³ According 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.	

¹ according to press release of the Czech railways of 2008/02/01, <http://www.ceskedrahy.cz/tiskove-centrum/tiskove-zpravy/-2169/>

² according to press release of the Czech railways of 2009/04/02 <http://www.ceskedrahy.cz/tiskove-centrum/tiskove-zpravy/-2698/>

³ see report of Edrigran of 2006/11/08 <http://www.edri.org/edrigran/number4.21/bba>

	<p>As a traffic inspectors in each train were equipped with a readers system allowed for tracking of the movement of individual passengers. NGO asked Czech railways to issue anonymous RFID cards and implement measures to prevent tracking the movement of its customers.⁴ 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 introduced system of season ticketing using chip cards and violated their responsibility of controller of personal data by not fulfilling their information commitments 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 individual 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.”⁵</p>	
Others	Card is currently serving as discount loyalty card in some theatres and since 2008 also as e-purse for rail tickets ⁶	
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	

⁴ 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

⁵ Czech Data protection authority Annual Report 2008, pp. 63 - 64,
http://www.uoou.cz/files/vz_2008.pdf

⁶ for details see english web pages of the project <http://www.inkarta.cz/eng-instrukce.aspx>

	adress (voluntary), telephone number (voluntary), date of the request, date of issuing the card, signature ⁷	
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 (!) ⁸	
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. ⁹ / 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 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. ¹⁰ / 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	„Controller declares it will anonymise personal data in its database 5 years	

⁷ 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>

⁸ 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>

⁹ see <http://www.inkarta.cz/>

¹⁰ 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>

Right to be forgotten	after last operation with this electronic financial tool. ¹¹	
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. ¹²	
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 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.	
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	

¹¹ quote from conditions of commercial use of In-karta, transl. F.P., <http://www.inkarta.cz/files/Obchodni-podminky.pdf>

¹² quote from conditions of commercial use, transl. F.P., <http://www.inkarta.cz/files/Obchodni-podminky.pdf>

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

	<p>disagreement with the processing.</p> <p>(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.</p> <p>Article 6</p> <p>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.</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</p>	

	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...)	<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 processing shall be:</p> <ol style="list-style-type: none"> 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. <p>Article 7 – Data security</p> <p>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.</p> <p>Article 8 – Additional safeguards for the data subject</p> <p>Any person shall be enabled:</p> <ol style="list-style-type: none"> 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; 	

	<ul style="list-style-type: none"> 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	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 recommendations 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	<p>Establishing a rule of obligatory introducing of anonymous cards instead of non-anonymous cards when possible</p> <p>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.</p> <p>Establishing a new legislation specifically focused on RFID.</p>	

Podpořili nás:





Lichtenštejnska a Norska v rámci

Finančního mechanismu EHP a Norského finančního mechanismu
prostřednictvím Nadace rozvoje občanské společnosti.