GUIDELINES REGARDING THE PROCESSING OF PERSONAL DATA BY MEANS OF SMART CARDS AND RFID TAGS

Component 2
Activity 2.1.4 - 4

Final Version – February 2012

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union
Contents

I. INTRODUCTION ................................................................................................................................. 3

PURPOSE/AIM OF THE DOCUMENT ..................................................................................................... 3
TECHNICAL BACKGROUND .................................................................................................................. 4
TO WHOM THESE GUIDELINES ARE ADDRESSED? ............................................................................. 4

II. DEFINITIONS .................................................................................................................................. 4

WHAT IS A SMART CARD? ................................................................................................................... 4
WHAT IS RFID TAG? ............................................................................................................................. 6
-----------------------------------------------------------------------------------------------
WHAT IS A SMART CARD? ................................................................................................................... 4
WHAT IS RFID TAG? ............................................................................................................................. 6

III. DATA SUBJECT’S RIGHTS .............................................................................................................. 8

WHAT DOES THE PRINCIPLE OF FAIR PROCESSING MEANS? .......................................................... 8
THE RIGHT OF THE DATA SUBJECT TO BE INFORMED ......................................................................... 8
RIGHT TO COMPLETE, CORRECT AND UPDATE THE DATA (PRINCIPLE OF ACCURACY) ...................... 9
HOW TO APPLY SECURITY MEASURES? ............................................................................................... 9
HOW TO EXERCISE THE DATA SUBJECTS’ RIGHTS? .......................................................................... 11
HOW TO EXERCISE THE RIGHT TO COMPLAIN? ................................................................................. 11

FAQ - FREQUENTLY ASKED QUESTIONS ............................................................................................. 12
I. INTRODUCTION

This code/guideline set the basic principles and guidelines for the effective protection of privacy with regard to the processing of personal data by means of smart cards and RFID tags in accordance with the Law on personal data protection (hereinafter “LPDP”).

Purpose/aim of the document

The purpose of these Guidelines is to explain the basic characteristics of smart cards, RFID and NFC technologies, to illustrate some of the dilemmas regarding processing of personal data in the context of the use of this technology, and to provide answers to frequently asked questions encountered by private and public sector subjects.

The Guidelines also specifies necessary requirements for fulfiling legal principles and data controller’s obligations to comply the Law on Personal Data Protection (LPDP) when smart cards and RFID tags technologies are implemented into a processing of personal data. The document also introduces some data protection problems in NFC (Near Field Communication) technology which is a new wireless communication technology intensively deployed in practice.

Protecting privacy and personal information means protecting individuals’ rights to control how personal information is collected, used, stored and passed on. Protecting privacy also includes information security—protecting the confidentiality, integrity and availability of personal information. To be considered privacy-secure, an identification system must be designed to satisfy both of these parameters. With the help of such explanations, answers and guidelines, companies and other data controllers and processors should accordingly be able to comply with the provisions and principles of the Law on the Protection of Personal Data (Official Gazette No.07/05 with amendments published in the Official Gazette under no. 103/08 and under no. 124/10; hereinafter “the LPDP”), international standards and principles and the EU regulations (Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

Smart cards are frequently used for various applications in current society. Smart cards are used in public transportation, banking operations, identification of citizens, health care services, and many more. These applications provide cardholders with greater control of their personal data flows and processing. The nature and capability of smart card technology creates many legal and ethical issues.

A smart card brings personal data processing more secure and provides opportunity to citizens greater control over the processing of their personal data. However, all advantages entail new problems that need to be addressed – e.g., who is owner of personal data used in the system; who is responsible for the accuracy and security of the data when the system is accessible to a number of other entities; where is the limit for sharing different applications into one smart card, where are risks to private life of individuals, and so on.
Smart card technology is essential to achieving lower costs, creating administrative efficiencies, improving communication between cardholder and data controller, increasing privacy, security and identity in general.

**Technical background**

In principle the smart card in a miniature computer without screen and keyboard. Smart card contains an embedded integrated circuit (chip) that can be in different technology (secure microcontroller with memory, cryptographic chip, etc.). Smart card technology conforms to international standards ISO/IEC 7816 and ISO/IEC 14443. Due to big capacity of the chip memory current smart cards can perform many functions, such as storing data, making calculations, processing data, managing files, and executing encryption algorithms. Smart cards make possible sophisticated and portable data processing applications which are reason that smart card application shall meet personal data processing principles set up by the Law on Personal Data Protection.

**To whom these guidelines are addressed?**

These Guidelines are addressed to data subjects and broad public informing them about processing of personal data with smart card technology and about fulfillment their rights given to them by the Law on Personal Data Protection. However, also data controllers, data processors and whatever companies who process personal data by the means of chip-base technologies will find useful information.

**II. DEFINITIONS**

Complete definitions of data protection legal area is mention in the text Law on Personal Data Protection. In this part are only terms which need to be added with explanatory text concerning the smart cards and RFID tags.

**What is a Smart card?**

The plastic card with a memory has been a part of peoples’ lives since 1950, when the Diners Club issued pay cards as members’ identification. The first plastic credit card was then issued by the Bank of America in 1960. Since that time, it has been used in various areas of human activity: in banking, business, health care etc. Later on, the card was equipped with memory elements which enabled the card to carry more and more data. The capacity of these memory elements increased along with developments in technology. The amount of personal data concerning cardholders also increased. This data serves as identification and also characterises the cardholder within the scope of the area for which the card was issued (health data, payment data, consumer data, etc.).
The "card" phenomenon complementary to the "net" one

Smart card is being considered as a tool specific to reasonable increase of the quality of today’s information society in general. The smart card phenomenon stands in opposition of the networks, especially open and unsecured but widely used Internet. The cards represent individualised sophisticated tools in comparison with commonly shared (but unique) network.

While smart cards are offering multiple functionality as, for example, digital signature, encryption and storage of selected information, networks provide universal access to information and knowledge. To achieve the optimal benefit for users/citizens, both technologies should be combined. Thus the synergies of cards and networks for advanced information society have to be analysed and recommendation for appropriate solutions have to be developed.

In this sense the dual platform of card + network paves the way towards the challenged applications and ought to be evaluated as complementary technology for both its benefits and risks.

Card as security enhancing tool - key holder/generator

Adequate and trustworthy use of the information and communication technologies represents a critical success factor to recent information society.

The smart cards ensure security features in very specific and individualised way: in one time they enable to capture private data related to the cardholder, but the computation facility is being added, so the access to the data content can be smartly controlled in various ways by cardholder and the information system.

Whilst in the past many projects tried to build their communication infrastructure either on cards or on networks, it is now widely accepted that some needs of security, privacy and universal access to patient data may only be achieved by combining the functions of smart cards and networks.

One of the essential features is the possible generation of cryptographic keys within the smart card itself. Together with the provision for electronic signature and enciphering and advanced standardisation make the smart card as unrivalled tool. It must be remarked that the GSM\(^1\) is often compared as potential competitor aiming to provide individuals with a mobile handset instead of a smart card. But GSM is in fact based on plugged smart card called SIM\(^2\) and the handset is nothing more than smart card and human interface. In this sense the rules and recommendation for card users and GSM users became identical.

\(^1\) GSM – Global System for Mobile communications
\(^2\) SIM – Subscriber Identity Module card
The use of cryptographic smart cards implies the setting up of public key infrastructures, where the access to relevant data won’t be possible without permanent access to these infrastructures. Hence internationally harmonised infrastructures have to be built and operated. The need for international interoperability by these measures is obvious.

Card enables effective off line transaction management

Beside the security, the smart cards bring also business-oriented advantage, which is the feasibility to provide secure off line transaction. This means mainly user authorisation – by means of that procedure the cardholder proof his relation to the card - and mutual authentication between the card and the information system to which the card has been connected.

The off-line operation is important for two basic reasons: firstly it makes certain solutions feasible saving costs of on-line required communication (and the real time in the same case) and it solves emergency cases in which the on line connection is not available for whatever reason.

On the other hand off-line procedures bring a new class of risks to be evaluated, related to off-line secure computation not supervised via enhanced powerful servers and with the security of authentication between remote off line running workplaces and network servers.

Smart cards provide sufficiently secure solution for those requirements.

The expected expansion of smart card applications anticipates the increase in personal data processing. With the growing amount of personal data being stored in a card’s memory, the risk of this data being growing and of the cardholder’s privacy being compromised increases. This Guidelines aim is to pay attention to these risks and to determine principles to ensure that these risks are minimised.

What is RFID tag?

Some definition of RFID provides Jonathan Weinberg, professor of Law, from Wayne State University: “The term RFID (or Radio Frequency IDentification) describes a family of technologies in which a “tag” contains an integrated circuit storing data that identifies or describes the tag itself, or the item it is attached to, or the person carrying it, and the data can be read, wirelessly, by a separate device called a “reader.”
In short, Radio frequency identification (RFID) is a technology that enables data exchange from a small, inexpensive, wireless device, called an RFID tag that is equipped with a computer chip and antenna. An RFID device can simply transmit its unique identification number; it can also transmit additional data about a specific object (e.g., date of a product’s packaging, price, factory of origin, etc.) or person (e.g., name, health status, etc.).

A Radio frequency identification (RFID) plays important role in a new development in the Information Society where objects equipped with microelectronics that can process data automatically will increasingly become an integral part of daily life. Although the technology has been used since the 1980s, it has become more widespread today due to advances in networking, miniaturization, and computing. Radio frequency identification (RFID) is a technology that allows automatic identification and data capture by using radio frequencies. The salient features of this technology are that they permit the attachment of a unique identifier and other information – using a micro-chip – to any object, animal or even a person, and to read this information through a wireless device.

Peter Hustinx, the European Data Protection Supervisor, says: "RFID systems could play a key role in the development of the European Information Society but the wide acceptance of RFID technologies should be facilitated by the benefits of consistent data protection safeguards. Self-regulation alone may not be enough to meet the challenge. Legal instruments may therefore be required to guarantee that the technical solutions to minimise the risks for data protection and privacy are in place."

RFIDs are not just "electronic tags" or "electronic barcodes". When linked to databases and communications networks, such as the Internet, this technology provides a very powerful way of delivering new services and applications, in potentially any environment.

The RFID tags are more and more used by businesses to monitor goods and governments are presently considering the introduction of these tags in ID documents. The RFID market will probably further grow spectacularly in the next years. The EU prediction is that more than 270 billion radio-frequency ID tags could be sold by 2016 in the world.

"The large majority are willing to be convinced that RFID can bring benefits but they want to be reassured that it will not compromise their privacy. This is the deal that we have to strike if we want RFID to be accepted and widely taken up", said Ms W. Reding on the EU Conference in 2006. The EU studies have shown that people need to have control on the information and decide on when and how the information is used or updated.

---

3 See EDPS Opinion regarding RFIF issued in December 2007
4 See the Communication document COM(2007) 96 final
The rights and obligations concerning the protection of personal data set up by Directive 95/46/EC and the Law on Personal Data Protection of beneficiary are fully applicable to the use of RFID applications that process personal data. It should be taken in mind that in all sector which implement RFID system, an assessment of the privacy and data protection impacts of services containing tags should provide the necessary information to clients (data subjects) to determine whether there is a likely threat to privacy or the protection of personal data.

### III. Data subject’s rights

**What does the principle of fair processing means?**

It must be reminded that if the smart card of RFID tag containing unique Identification (ID) is destined to be carried by a person, then the card/RFID tag ID should be considered as personal data. Than, all data protection principles shall be apply to this ID. If the smart card or RFID technology is used for fulfilment of specified purpose(s) than it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded.

Smart cards offer not just a number of advantages in electronic communication, but they also entail risks for private citizens, particularly due to the fact that they make it possible to map out the transactions performed and thus to monitor the private life of their holders. These facts generate many legislative questions. In using smart cards it is often unclear who is the “owner” of the personal data recorded on the card, who is responsible for their completeness and accuracy, who is responsible for card and system security.

In using smart cards as a technology used for personal data processing, it is necessary to stipulate legislative, ethical and other rules for the protection of such data from unauthorised access, modification, publication or any other unauthorised processing. The extent and severity of these rules grow with the number of applications for which the personal data are used (multi-application). The multi-application use of a smart card entails an increasing aggregation of personal data on the card and hence also the risk of its abuse and the risk of unauthorised monitoring of personal privacy.

**The right of the data subject to be informed**

---

Where personal data are collected and stored on a smart card, the data subject should be informed of the purposes of processing, the identity of the controller, the categories of data concerned and the recipients or categories of recipients of the data that are stored. Other information should be provided to the data subject, where this is necessary to guarantee fair processing of personal data.

The personal data subject may anytime request from the controller to inform him/her on the scope of personal data or categories of processed personal data related to him/her, on the purpose(s) of processing personal data, means of processing (see articles 10, 11, 12 of LPDP).

Information to data subject must be provided in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors. When a card is issued, the card holder should be properly informed about how to use his/her card and what to do in case of fraud or unauthorised disclosure.

Whenever personal data are exchanged between a smart card and the system, the data subject should be alerted (eg. sound signal), unless he/she already has this information. This is particularly important in the case of contact-less cards, that is to say if the data subject does not insert or present the card to the system him-/herself.

**Right to complete, correct and update the data (principle of accuracy)**

The principle of accuracy means that personal data collected and process by chip-base technology shall be accurate and, where necessary, kept up to date. Personal data, which is inaccurate, incomplete, or not up to date having regard for the purpose for which it was collected or for which it is processed, is erased or rectified. Personal data stored in smart card memory shall be fully updated.

Upon the request of the personal data subject, the controller is obliged to supplement, amend, delete or prevent the use of the personal data, if they are incomplete, incorrect or not updated and if their processing is not in conformity with the provisions of the Law (article 14 of LPDP).

If controller determines that the personal data are incomplete, incorrect or not updated, responsible person of the controller is obliged to supplement, amend or delete them, regardless of whether the personal data subject has submitted a request for amending the personal data.

For the performed supplement, amendment or deletion of personal data, the controller shall be obliged within 30 days from the day of accepting the request, to inform in written the personal data subject, the personal data users or third parties to whom the personal data have been disclosed to, unless it is not possible or it quests for disproportional effort or costs.

**How to apply security measures?**

In order to provide secrecy and protection of the processing of the subject’s personal data, the controller and processor have to apply proper technical and organizational measures for protection of accidental or illegal damaging of the personal data, or their accidental loss, change,
Unauthorized disclosing or approach, especially when the processing includes transmission of data over a network and protection of any kind of illegal forms of processing. Those measures have to provide degree of protection of the personal data appropriate to the risk during the processing and the nature of the data being processed.

The controller and processor are be obliged to adopt and apply documentation containing description of the technical and organizational measures for providing secrecy and protection of the personal data processing.

Security measures include, among others, security of the buildings in which the personal data are stored and/or processed (including access to the building), list of authorised persons (with a mention of their liability) to access the data, appropriate authentication mechanisms (e.g. passwords control), and security in the transfer of data between the data controller and the data processor.

Controllers should satisfy themselves that any processors they employ have appropriate security measures (including respect for confidentiality) by including appropriate provisions in the contract.

The obligations with regard to the protection of personal data fall upon the person who determines the purpose of the system and the means that are used to fulfil this purpose. This implies, in the case of a multipurpose card, that different controllers are each responsible for their part.

Data recorded on a card should be protected against any unauthorised or accidental access, alteration and/or erasure. The card should offer an appropriate level of security given the state of technology, the sensitive or non-sensitive nature of the data recorded, the number and type of applications and the evaluation of possible risks. The conditions under which third parties may have access to data recorded on the card should be established beforehand for each of the separate purposes for which the card is used.

**Whole security framework of each smart card application has following parts:**

**Technology security** – is about reliability, technical solution, quality of components used in the system, resistant to breakdowns and attacks as well as respect of international norms defined by relevant standardisation bodies (eg. CEN - European Committee for Standardization, and ISO - International Standard Organization). This part of security framework is ensured mostly by card industry. However, issuer of the cards is obliged control if all these technology are properly applied. The card system controller (incl. data controller) has influence to this part of security framework by his activity linked to selection of the best quality technology suppliers. Controller practically hasn't direct influence to quality of products.

**Application security** – requested level of security in whole system (application). *Risk management, risk analysis. Impersonation* (a risk that unauthorized person misuse function of the card), *Repudiation* (an issue related to authorization of correct way during transmission of data) are issues which data controller and the application system controller must ensure.

**Protection of data** written into chip, authorization access right to data, protection against unauthorized reading, modification, misuse of data;
**Legislative and ethical issues** (i.e. legal aspects of application, respect of EU, Council of Europe and domestic legislation (laws, recommendations, etc.) are a part of responsibilities and reliability of data controller and application controller shall guaranteed.

Security frame of smart card and RFID application is an important key to successful solution of the system as a whole.

**How to exercise the data subjects’ rights?**

The data subjects’ rights as defined in the Law (LPDP) other regulation and this code/guidelines, including the right to object to the processing of his data for specific purposes including the possibility of not being contacted on behalf of someone else, object to the disclosure of data to a third party, access and to rectify data which are inaccurate, to claim the deletion or blocking of data when its processing does not comply with the provisions of the applicable legislation, to object the processing of data for different purposes, shall be exercised in the first instance before responsible person/officer of the data controller or processor, directly or through a representative.

The responsible person/officer must implement procedures to enable data subjects to exercise the rights provided in the law and/or this code/guidelines in a simple, fast and efficient way, which do not entail undue delay or cost nor any gain whatsoever for the responsible person.

When a responsible person concludes that pursuant to the law the exercise of rights under this code/guideline is not justified, the data subject should be informed of the reasons that led to this conclusion.

**How to exercise the right to complain?**

Whenever one believes that her/his right of personal data protection is violated and has some facts or prove for the violation, s/he can submit to the Directorate for Personal Data Protection:

- Request (complaint) for determining a violation of the right of personal data protection or
- Initiative to the the Directorate to perform inspection over the personal data processing performed by the controller of personal data collection.

In order to facilitate these procedures, the Directorate has developed forms of Request (complaint) and the Initiative for performing inspection, which are published on the Directorate’s web site (www.privacy.mk/mk/prijavi zloupotreba).

After filling the required information in the Request (complaint) or Initiative for performing inspection you can easily submitted via following e-mail: contact@dzlp.mk, contact@privacy.mk or by ordinary mail. The whole procedure is in details explained on the aforementioned Directorate’s web site (www.privacy.mk/mk/prijavi zloupotreba).
FAQ - Frequently Asked Questions

1. **What is a difference between smart card and chip card?**

Chip card is a synonymous of smart card. Smart card is often called chip card or integrated circuit (IC) card. Some experts prefer to reserve smart card for microprocessor card (integrated circuit is a microprocessor chip) and other expresses for memory cards (integrated circuit is a memory chip).

2. **How the cardholder can make sure that data in the chip are correct and right?**

Each card issuer (data controller or the system operator) guaranties cardholders using the card properly. Next to this guaranty everybody can recognize the level of security which corresponds to the issuer responsibility.

3. **What is a contactless smart card?**

A contactless smart card includes an embedded smart card secure microcontroller or equivalent intelligence, internal memory and a small antenna and communicates with a reader through a contactless radio frequency (RF) interface. Contactless smart card technology is used in applications that need to protect personal information and/or deliver fast, secure transactions, such as transit fare payment cards, government and corporate identification cards, documents such as electronic passports and visas, and financial payment cards.

Contactless smart cards have the ability to securely manage, store and provide access to data on the card, perform on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a contactless smart card reader. Contactless smart card technology and applications conform to
international standards (ISO/IEC 14443 and ISO/IEC 7816). Contactless smart card technology is available in a variety of forms - in plastic cards, watches, key fobs, documents and other handheld devices (e.g., built into mobile phones).

4. Can somebody misuse my card if lost or stolen?

There is no difference between this card and any other passport concerning basic and public identification features. Your sensitive medical data, however, are accessible only on your personal authorization or for predefined health professionals (similarly your paper medical file).

5. The smart card with processor is relatively expensive. Why don’t you use a magnetic card?

Magnetic card can not capture sensitive personal data because of lack of space and security. Such card can be used like a key to the database. However such scheme requires interconnection each time you use this card, and it is costly and time consumption procedure if secure. Generally speaking, the magnetic card is very limited for the use due to lack of security measurements.

6. I have heard that it is possible to have only one card for many purposes and functions. Why you have issued this card only for health and social security using?

It is called multi-application (or multi-function) card system. But such a system must be very carefully designed when personal data is processed in the system. Up to now so called related applications are considered. The relation is given by similar purpose and usage of the card. Let us consider, as example, how easy a medical card can be damaged by daily use in canteen or payphone, while for medical service could be used for years because it is presented seldom. If damaged, medical card has not only to be reissued, but all the data has to be reloaded by GP.

7. What are some of the most common applications for RFID?

The most common applications are payment systems, access control and asset tracking. Increasingly, retail, apparel, aerospace, defense, manufacturing, consumer packaged goods and pharmaceutical companies are looking to use RFID to track goods within their supply chains. Health care providers, energy producers and construction companies are using active RFID system to track large equipment, tools and vehicles. RFID is implemented in e-Passports, e-Identity documents and many more.

8. From how far away can a typical RFID tag be read?

The distance from which a tag can be read is called its read range. Read range depends on a number of factors, including the frequency of the radio waves uses for tag-reader communication, the size of the tag antenna, the power output of the reader, and whether the tags have a battery to broadcast a signal or gather energy from a reader and merely reflect a weak signal back to the reader. Battery-powered tags typically have a read range of about 100 meters. These are the kinds of tags used in toll collection systems. High-frequency tags, which are often used in smart cards, have a read range of three feet or
less. UHF tags-the kind used on pallets and cases of goods in the supply chain-have a read range up to 10 meters under ideal conditions. If the tags are attached to products with water or metal, the read range can be significantly less. If the size of the UHF antenna is reduced, that will also dramatically reduce the read range. Increasing the power output could increase the range, but most governments restrict the output of readers so that they don't interfere with other RF devices, such as cordless phones.