INFORMATION COMMISSIONER
Vošnjakova 1, p.p. 78, SI-1000 Ljubljana
Phone: + 386 (0) 1 230 97 30
Fax: + 386 (0) 1 230 97 78
www.ic-rs.si
REPUBLIC OF SLOVENIA

Date: July 14, 2008

Opinion of the Information Commissioner on the protection of personal data in the electronic road toll system

The Information Commissioner, pursuant to subpara 7, Par 1, Art. 49 of the Personal Data Protection Act[1] (Official Gazette RS, No. 94/07 – official consolidated text; hereinafter : ZVOP-1-UPB1) and Art. 2 of the Information Commissioner Act (Official Gazette RS, No. 113/05 and 51/07 – ZUstS-A, ZInfP) hereby issues a non-mandatory opinion on the problems of personal data protection in electronic road toll system for private cars. It needs to be stressed that we have not received any request for issuing the opinion on this matter, however, considering the fact that the electronic road toll system entails quite substantial processing of personal data, we believe this opinion is necessary and it is expected that the proponents of legislation and tendering procedures will take it into account. The Information Commissioner, as a national supervisory body, is also authorised under Art. 48 of ZVOP-1-UPB1 to issue prior opinions to Ministries, the National Assembly, self-governing local community bodies, other state bodies and holders of public powers, regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations regulating personal data.

Current standards on personal data protection within EU have been laid down by the Directive 95/46/EC of the European Parliament and of the Council of Oct

[1] Unofficial translation into English is available at: http://www.ip-rs.si/index.php?id=339

24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (UL L 281, Nov 23, 1995, with amendments, hereinafter: Directive 95/46/EC), the Directive of the European Parliament and of the Council 2002/58/EC of July 12, 2002 on personal data processing and the protection of privacy in the field of electronic communications (OG L 201, July 31, 2002, hereinafter: Directive 2002/58/EC) and by the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (hereinafter: Convention 108). The right to personal data protection is also explicitly recognised by Art. 8 of the Charter of Fundamental Rights of the European Union.

Directive 95/46/EC, Art. 6 sets out basic principles on the quality of data, meaning that personal data must be: (a) **processed fairly and lawfully**; (b) **collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes**; (c) **adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed**; (d) **accurate and where necessary, kept up-to-date**; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) **kept** in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the data were collected or for which they are further processed. The administrator of personal data must ensure that the data are processed in accordance with these requirements.

The Directive of the European Parliament and the Council 2004/52/EC of April 29, 2004 on the interoperability of electronic road toll systems in the Community (OG L 166, of April 30, 2004, hereinafter: Directive 2004/52/EC),

Par 7, Art. 2. stipulates that member states must ensure that personal data used for European electronic road toll system are processed according to the rules of the Community on the protection of freedom and basic rights of individuals, including their privacy, and in particular, respecting the provisions of directives 95/46/EC and 2002/58/EC. The Directive 2004/52/EC also explicitly sets out legal issues which need to be addressed: among others the need to authenticate the validity of the selected technical solutions in relation to the rules set out by the Community which protect the freedom and basic rights of individuals, including privacy, and in particular to ensure conformity with the two directives mentioned above.

In the Republic of Slovenia these provisions have been concretised by the Constitution and by ZVOP-1-UPB1. Under its authority and mentioned privacy standards the Information Commissioner wants to primarily emphasize the fact that due to inadequate technical and legal arrangements the system of road charging **might lead to impermissible and excessive collection and processing of personal data**. Therefore, from the aspect of lawful and fair processing of personal data in accordance with ZVOP-1-UPB1, and to ensure the respecting of principles of purpose and proportionality of processing and collecting of personal data under ZVOP-1-UPB1 it is of utmost importance that the legislator needs to clearly define which personal data should be collected, and the purpose of collection, and to define a narrow scope for the collection and processing, necessary for achieving legally defined aims and purposes for which the data will be collected. In electronic road toll system this means selecting corresponding technical solutions which would support the implementation of legally defined aims **without unnecessary and excessive processing of personal data**. Further on the Commissioner presents her opinion on the issues from the aspect of personal data protection before introducing the electronic road toll system.

It needs to be emphasized that electronic road toll system in transportation involves processing of a **significant amount of personal data**, that is the information on the **position** and **journey time** on the driver's route. The aim of the Directive 2004/52/EC is to follow the »pay as you go« principle. Also, the trans European system should provide toll charging for all types of roads on which tolls are charged, including viaducts, tunnels and other objects, which means that the systems will require processing of all personal data mentioned before. With the new road charging system drivers could pay the toll without any stopping in congesting traffic. Also, the same device would allow paying the toll on all European motorways, which would be defined as payable. Directive 2004/52/EC envisages two possible technologies to support the system: short range communications (DSRC[2]) and global navigation satellite system, which can determine the position of the car and transmit the data via high-performance wireless communication networks (GNSS/CN[3]) – the latter is frequently referred to as satellite toll system. Both technological options are admissible. Each has its advantages and disadvantages: microwave technologies, for example, are more widely used and tested but they are not suitable for all roads. The advantage of the satellite toll system is its flexibility, while on the other hand this system has not been tested enough in Europe. Here we need to emphasize that there should be no concern that such satellites would have an all encompassing database on the position of vehicles – the GPS as well as the future Galileo are based on passive receivers, which only calculate the location of the vehicle from the data received from satellites, and these receivers can not communicate the information on the location of the car to satellites. Therefore, in opting for the system of satellite toll charging we need to consider that by satellite navigation a vehicle obtains only the information on its position, while the data are transmitted via wireless networks

[2] Dedicated Short Range Communications.
[3] Global Navigation Satellite System/Cellular Networks.

to the control toll charging centre, as for example GSM network.

In questions of personal data protection in electronic road toll system the following issues need to be considered:

1. characteristics of the device for calculating the fees due,
2. optional or compulsory use,
3. sharing the roles and responsibilities in the system of charging the toll,
4. surveillance over committed violations.

In order to ensure the privacy of individuals, the most appropriate system would be the one in which the data, needed for the purpose of toll service, **would be exclusively under the surveillance of the user**. In this case the calculation of the toll would be made by the device[4] (the so called intelligent device or Smart Client), while the control centre would receive only the **sum of the toll spent**. This means that all four phases of the calculating procedure in electronic road toll system would be processed by the device itself:

1. determining the position of the vehicle,
2. determining the segment of the road and the corresponding tariff,
3. calculating the sum spent for that segment,
4. sum total.

By this variant the **anonymity of the driver would be preserved since all the data on the position and journey time would be kept under sole control of the user**. The users should identify themselves only if certain irregularities emerged in which identification would be required: for example, when the user has not paid a correctly calculated toll fee, or when the vehicle

[4] OBU (on-board unit).

has been stolen, when the user's toll system device is broken down or malfunctioning (whilst driving on a charged road segment). All that is needed to ensure is that the device in the vehicle which calculates the toll is working correctly on the roads on which tolls are charged. This system, of course, also requires some safety precautions. It is necessary to provide suitable certification standards, proper installation and maintenance of such devices, and also consider some technical aspects (e.g. power supply, checking correct functioning), and costs (a smart device is definitely more expensive). In such system the control centre does not have data on the position of the vehicle; it only checks whether the device is operating correctly. This solution has certain economic advantages: this »intelligent« device is not sensitive to communication hindrances, e.g. areas which are not covered by GSM signal, or if the clearance (i.e.control) centre is temporarily not operating since the system can process the toll itself. On the other hand, the device which continuously sends data (the so called Thin Client) to the clearance centre cannot process the calculations of the toll by itself in the areas which are not covered, or when the central control is not working. It is also important to mention that the intelligent device also supports operation in the »Thin Client« mode, which is a requirement for the interoperability within Europe. The devices in vehicles will need to know how to respond to different regimes: after entering a territory of another operator, the device will receive instructions how to work. According to the information available to the Commissioner, international standardisation organisations ISO and CEN are developing suitable technical standards, while the industry, or potential manufacturers, already have proven working solutions.

The Commissioner believes that on the territory of R Slovenia, and in view of the principle of proportionality of personal data processing, the calculation of the toll should be made by the unit itself. **With all the above, the**

Information Commissioner believes, that only such distribution of toll charging process, by which the data are kept in the sole possession of the individual, can satisfy the criterion of proportionality in processing personal data (Art. 3 of ZVOP-1-UPB1). The basic principles of personal data protection are characterised by **the principle of purpose of use** and **the principle of proportionality**, and they derive from the postulate that any personal data processing in fact means encroaching into the constitutional right to privacy. For this reason, only such amounts of data should be collected and further processed which would be necessary for achieving a certain aim. If the aim is an efficient and fair toll collection (and this is what all the parties involved keep emphasizing), it is believed that the method described above is the one which can meet these criteria. Other solutions can not satisfy the proportionality criteria if there is an alternative method which ensures lesser encroachment into the privacy of individuals.

A more privacy invasive approach, **which already does not satisfy the proportionality criterion**, is a solution based on the principle of sharing the data between two centres, where one centre has the identification number of the device in the vehicle and receives information on the route the vehicle has made (journey time and position), but does not know who the owner of the device is. Based on this information the centre calculates the fees due (this centre can also be merely a technical centre – a kind of an intermediate or proxy which has been selected to perform calculations). Such aggregated calculations of data (only the sum of the toll within a certain time period, without information on journey time and position), are then sent together with the identification number of the device to another centre which can identify the owner of the device who is then charged with the toll, however, this centre does not keep the information on the journey of the vehicle. This solution **only apparently protects the privacy of in individual**, even though one centre

keeps the information on the vehicle position and journey time and does not know the identity of the driver, and vice versa. In this way there are still **enormous amounts of personal data collected and processed centrally,** by one centre (data on journey time and position). The Article 29 Working Party and the Information Commissioner both share the same view, namely that data, relating to an identified or identifiable natural person, need to be treated as personal data[5]. **The identifiability of an individual is not assessed only through the means and resources of a data controller (in this case the first centre) but should rather be assessed in general.** The controller anticipates that the "means likely reasonably to be used" to identify the persons will be available e.g. through the courts appealed to (otherwise the collection of the information makes no sense), and therefore this information should be considered as personal data. Regardless of whether the first centre can or cannot identify an individual to whom the data on time and position refer to by itself, this centre **undoubtedly processes personal data**: pursuant to indent 1, Art. 6 of the ZVOP-1-UPB1 the meaning of personal data is any data relating to an individual, irrespective of the form in which it is expressed. By indent 2 of the same article, an individual is an identified or identifiable natural person to whom personal data relates; an identifiable natural person is one who can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time. To support this, it is evident that in case the road charges have not been paid, or the person has refused payment, the creditor will need to find a quick and simple way to reproduce the calculation of the toll which means that the data on journey time and position of an

[5] See Article 29 *Opinion 4/2007 on the concept of personal data,* accessible at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_sl.pdf.

identifiable person will need to be processed).

A simple weighing by the principle of proportionality proves that **the solution where the data are processed by two centres is worse than if personal data were exclusively under the control of the user. For this reason it is necessary to opt for the solution which means lesser encroachment into the constitutionally protected right of individuals to privacy.**

The least favourable solution for electronic road toll system in terms of the protection of privacy is that all data on journey time and position of vehicles are collected by a single body or institution, the data are kept in a centralised database separately by each user, while the purpose of using such data, security, and the number of users remain unidentified or unclear. Privacy advocates clearly will not support this solution; the Information Commissioner and other data protection authorities are frequently dealing with the so called *function creep* phenomenon, meaning that data are first collected for one purpose (which can be quite legitimate and lawful), however, later the same data are used for another purpose, access is possible by previously unknown third parties and so on. We can draw analogy with the previous case, where the data are shared between two subjects. The opponents of this argument will claim that if data were kept centrally and protected by suitable data security mechanisms (e.g. appropriate access control, tracing the manipulation with data, etc.), it would be possible to ensure a higher level of security than a single individual could ensure. A counterargument should be that even if better security was provided, we cannot disregard the fact that in case the data are under the control of an individual only his own personal data remain exposed, (e.g. if the vehicle, or the toll system device has been stolen), while in the centralised data keeping system personal data of all individuals are potentially exposed (in spite of a possible higher level of security). For this reason, and

from the viewpoint of privacy protection, it is necessary to favour such solutions where **personal data are not kept centrally (no matter whether the data with identity information are kept together at one centre, or exist in two separate centralised data collections), but remain in the possession and under control of an individual.**

The question of optional or compulsory use of the toll system device is to a great extent closely related with the question of surveillance because of the impacts on privacy. Taking into account that final decisions are in the discretion of individual member states. In principle, optional use is more user-friendly since individuals can give prior consent to processing their personal data (which is similar to the previous ABC[6] system); however, there is a problem with the surveillance of such use. An example from German experience for heavy vehicles (Toll Collect) shows that 90% of truck drivers have opted for the installation of a satellite toll system and less than 10% prefer other systems (e.g. by subscribing and paying the toll on the automatic station). The reliability and accuracy of the installed systems is 99.75% which means that all problems of surveillance and irregularities occur with those who subscribe and pay manually at toll stations (vehicles without installed devices). If we transfer German experience of heavy vehicles to the toll system for private cars to be eventually used on all motorways, the optional method would be problematic in a real situation. An optional toll system in a free flow traffic would require installation of very complex and expensive control systems on all payable roads (video surveillance, identification of number plates, etc.), which would consequently mean even greater encroachment into the privacy than in a compulsory system. Therefore, the decisions on the part of the initiators of the law need to be taken with great caution. For this reason, the Commissioner believes that the use of **alternative mechanisms of paying tolls should be**

[6] DSRC solution that was used in Slovenia.

at least destimulating. Frequently, comparisons are made with mobile telephony, however these two are incomparable: toll system devices (on payable roads) cannot be disabled like mobile phones (even if we freely decide to use such a device), and for this reason suitable personal data protection becomes even more relevant.

Special attention should be paid to the questions of **complaints** and **remote access to raw data by the surveillance centre, or third persons** in spite of the fact that the data are stored in the device and the device calculates the toll. If we really want to ensure that personal data remain under the user's control, it is necessary to provide access to the data only if the user explicitly requests so, while every access to the information on the position, journey time and tolls, needs to be suitably recorded, allowing an authentic and complete auditing tracing. It would be totally impermissible to allow unauthorised and unregistered access to the data in the device. The Commissioner wants to bring attention to the provisions under subpara 5, Par 1. and Par 2 of Art. 24 of ZVOP-1-UPB1, which stipulate that within the measures and procedures for the security of personal data, the database controller always needs to ensure that it is **possible to find out when the information about an individual was entered into the filing system, used, or otherwise processed and who did do so** for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data. In cases of processing of personal data, accessible over telecommunication means or network, system software and software applications must ensure that the processing of personal data in the filing systems **is within the limits of authorisation of the data recipient.** With this in mind it would be necessary to define, either in the proposal of the law or by adequate executive regulation, in what way the authorised person, who has access to such personal data, could access the data and identify an individual.

An individual (data subject) has the right of access to his own personal data, not only upon the request in cases of complaint, but also under the provisions of Art 30 of ZVOP-1-UPB1, which set out the legal rights of individuals to examine their own personal data. This right is one of the basic rights to personal data protection, laid down by Par 3, Art. 38 of the Constitution of RS, by which every person has the right to be informed about the personal data which refer to him, and should have the right to judicial protection if his data were abused. Art. 30 of ZVOP-1-UPB1 (indent 3, Par 1) stipulates that personal data controller must, upon the request of the individual, supply him an extract of personal data contained in the filing system that relate to him. With this provision the individual can request only the data which specifically relate to him.

The legal basis for introducing electronic road toll system for private cars will have to precisely define the **duration of storage of personal data** and **methods of accessing the information** which is stored in the device in the vehicle. According to the provisions of Art. 21 of ZVOP-1-UPB1 personal data may be stored for as long as necessary to achieve the purpose for which they were collected or further processed (after the toll has been charged). However, regarding the amount of personal data and the level of encroachment into the privacy of individuals caused by providing such access, the Information Commissioner believes that access to these data should be adequately limited with specific safeguards in place, and should be similar to legal protection for traffic data in electronic communications, which are stored under the provisions of the so called Data Retention Directive, transposed into Act on Electronic Communications[7]. Access to traffic data is meticulously regulated and possible

[7] Directive 2006/24/EC of the European Parliament and the Council of March 15 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

only upon the injunction of a competent body and only for the purposes which have been predefined and enumerated. At this point it needs to be emphasized that any restriction of the rights of data subjects' access to their own personal data should be explicitly stated in the statute governing the electronic road toll system for private cars, and this restriction of the right should be in agreement with the provisions of Art 36. of[8] ZVOP-1-UPB1.

An area where possible abuse of personal data may happen, and requires special attention, is the **implementation of surveillance and detection of offenders**. The Commissioner believes that the identity of the drivers must not be ascertained before the driver has committed something which is defined as a violation of the toll collection system. Here, it is necessary to consider the fundamental principle of proportionality, i.e. **first of all it needs to be established whether the toll system device is present in the vehicle and whether it functions faultlessly.** If the supervising unit does not detect any violations regarding the presence or proper functioning of the toll charging device, it should make no further steps for the identification of the device and the driver. Only, when the supervising unit detects the absence of the device, improper functioning of the device, or that some adjustments on the device have been made, the authorised body may, according to the principle of proportionality, proceed with number plate recognition process and thus identification of the individual, being the method that is, according to the reports of expert groups, an advisable method of control.

---

(1) The rights of an individual from the third and fourth paragraphs of Article 19, Articles 30 and 32 of this Act may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.

(2) Restrictions from the previous paragraph may only be provided in the extent necessary to achieve the purpose for which the restriction was provided.

The Commissioner also wants to draw attention to keeping extreme caution in managing the so called **blacklists** of offenders in automated number plate recognition. To understand the effects of encroachment into the privacy of individuals it is important to understand the situation, or circumstances of functioning of such system, particularly the **circumstance of the identification of individuals**. If the identity of the owner of the vehicle is revealed immediately after the number plate has been identified this would have completely different effects on the driver's privacy, than in the case when the identity of the car driver was established after a criminal offence has been made. Further on we present the experience of some other countries in introducing the system for **Automatic Number Plate Recognition (ANPR)**. Of course, in interpreting the data below, it is necessary to consider the different circumstances in which the system was introduced, and how the system operates:

- aim of use,
- scope of access to data,
- duration of storage of the data,
- moment and conditions for the identification of individuals,
- hit/no hit principle, etc.

According to the research carried out by the Dutch data protection authority (College Bescherming Persoonsgegevens - CBP) among national authorities for personal data protection, the automatic number plate recognition system is already used by 12 European countries (Bulgaria, Czech Republic, Finland, Hungary, Great Britain, Germany, Austria, Sweden, Ireland, Estonia, France and Lithuania), while in six countries (at the time the research was made: March-April 2008) this system was not in use (Belgium, Iceland, Denmark,

Portugal, Malta and Slovenia). The remaining nine countries did not respond to the questionnaire. In the majority of these countries such systems are used for the purposes of enforcement (searching stolen cars, or performing general investigations, detection of criminal offences and criminal prosecution). The research shows that the majority of countries are using the **hit/no hit** system. The system has been implemented in the majority of countries without any new legislation. According to the research, these countries consulted their own authorities for personal data protection. With this the Information Commissioner invites competent ministries to consult the Commissioner on these matters. The Commissioner, pursuant to Art. 48 of ZVOP-1-UPB1, has an authority to issue prior opinions to Ministries, the National Assembly, self-governing local community bodies, other state bodies and holders of public powers regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations governing personal data.

Considering all the above, it is impermissible to process personal data of drivers who have not committed any offence. With this approach, the supervising centre would only check if the device in the car has been functioning correctly, and only an authorised person (for the purpose for which this person has been given authorisation to access personal data) may request identification of the individual or obtain information on the position of the vehicle. This can be allowed only in certain circumstances which need to be predefined and enumerated (for example if the electronic toll system device in a car has been modified in such a way that it does not work properly, or if the device was not working while using payable roads, or if the car was stolen). Therefore, in order for the **toll enforcement** to be effective, it is **not necessary to reveal the identity and position of every driver in advance, but only in specific cases (these cases need to be legally set out)**. The proposal of the law should precisely define in which cases the

individuals, or journey times, and position on the driving route should be identified. Also, it should be provided by law which authorised persons could process these data. The Commissioner also notes that personal data in the public sector (e.g. police), can be processed only if laid down by the statute. The statute may also stipulate that certain personal data can be processed only upon previous consent of individuals. This means that an explicit legal basis should exist for the police to process personal data in which (according to the principle of proportionality), the reasons and the purpose for collecting the data should be clearly and precisely set out, and the data to be collected precisely defined.

To conclude the opinion, the Information Commissioner believes that in relatively uncertain circumstances where final decisions will be taken at the European level, the position of Slovenia on electronic road toll system should be extremely carefully thought out. We cannot allow the adoption of such legislation and select a model which will later not comply with European standards. **Therefore, from the aspect of data protection, and in a situation where final decisions are still not clear, it is necessary to assume a standpoint which would ensure the adoption of highest standards for the protection of privacy, and which could in the given situation serve as a privacy enhancing approach in a broader European toll collection system**. This means we need to insist on suitable functional requirements which would support the implementation of legally defined aims in such a way that all the data on the position and journey time of vehicles would be stored under sole possession of the user avoiding centralised and unnecessary or excessive collecting and processing of personal data. Access to data limited to authorised persons, access audit logs for data integrity and traceability of data processing, personal data under sole control of the user and no disproportionate control mechanisms should ensure that electronic toll

collection is carried out in a privacy protecting manner.

In principle, the question of personal data protection in electronic road toll system is quite simple: basically, toll collection system does not require a centralised personal data processing system (as long as no offence has been committed), nor does it require disproportionate processing of personal data, access to personal data and ubiquitous surveillance. The fundamental principles of personal data protection strive for maintaining the anonymity of the driver, which means that the selected technology should help preserve this situation. Any digression from this principle would represent an additional encroachment into already eroded privacy in the information society, and encroachment into constitutionally protected rights of the individual.

Respectfully,

Information Commissioner:
Nataša Pirc Musar, LL.M.