

z2008-01050

Advice of 30 September 2008 on the legislative proposal on the “kilometre price”

The Minister of Transport, Public Works and Water Management requested the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)], in accordance with Article 51(2) of the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act], to issue recommendations on the privacy aspects of the kilometre price legislative proposal.

1. Contents of the proposal

The object of the kilometre price legislative proposal is to ensure increased accessibility of the living environment and to improve the related quality of the living environment. It is therefore advisable to introduce a price for driving a motor vehicle that depends on how much it is used. The introduction of the kilometre price means that the owner will no longer pay for owning a motor vehicle, but rather for using it. Simultaneously, the motor vehicle tax and the Private Motor Vehicle and Motorcycle Tax will be – gradually – phased out. The costs of use will be differentiated by time and place and environmental characteristics.

The Explanatory Memorandum (EM, page 6) lists seven preconditions set by the Government on the introduction of the kilometre price. These preconditions are:

1. Introduction of the kilometre price concurrent with proportionate repeal of fixed motor vehicle taxes: neutral as regards charges;
2. Proceeds to go to an infrastructure fund concurrent with proportionate reduction of the contribution from the general resources to this fund;
3. Affordable for road users;
4. No unnecessary administrative burden;
5. A transparent, user-friendly and reliable system;
6. Data protection:
‘The use of an electronic collection system, whereby personal data of road users are registered, demands – partly in view of privacy aspects – extra attention for the protection of the personal data of the road user.’ (EM, page 7);
7. Support by society for the proposal.

The introduction of the Kilometre Price Act is expected to take place in 2011 for freight traffic and in 2012 for passenger transport.

2. Assessment

Before proceeding to the assessment of the advice, please find below a brief historic overview relating to the involvement of the Dutch DPA in the kilometre levy/kilometre price file.

I. History

- a. Legislative advice 2001

In 2001, the Dutch DPA (and its legal predecessor the *Registratiekamer*) twice issued recommendations¹ on the Kilometre Levy Act, which was ultimately never introduced. The fact that a road pricing system may lead to a detailed picture of the movements of individual road users and the risk of unregulated/undesirable additional use were major causes for concern.

b. Legislative advice 2006

In 2006², the Dutch DPA issued recommendations on the amendment of the *Wet bereikbaarheid en mobiliteit (Wbm)* [Access and Mobility Act]. The Wbm provides for the possibility of introducing toll levying and a kilometre levy. The Dutch DPA conclusions included the following:

'The Dutch DPA is of the opinion that, to the extent it is necessary to process personal data, it is perfectly feasible, irrespective of the technology and/or collection agency to be elected, to formulate in advance a specific set of requirements concerning the protection of personal data.'

and

'The Dutch DPA considers it important that indications are provided in advance as to which forms of processing are necessary for which purpose; data minimisation should serve as the starting point (Article 7 of the Wbp). In the case of consent (Article 8, at a, of the Wbp), it must also be certain that it is independent of attractive (more attractive) rates.'

c. Hearing of 31 January 2008

The Government sent the *Anders Betalen voor Mobiliteit (ABvM)* [Paying Differently for Mobility] policy programme to the Lower House at the end of 2007. Pursuant to the above, the Permanent Committee on Transport, Public Works and Water Management organised a hearing. The Dutch DPA was allowed to present its views during the hearing. The Dutch DPA's views were also stated in two letters³ to the Permanent Committee. The Dutch DPA's main positions are:

1. From the perspective of adequate protection of personal data, the 'thick' variant (the On Board Unit – OBU – whereby detailed travel information is only available to the owner of the vehicle) of the registration system qualifies as the most acceptable variant: only those personal data are processed that are necessary to charge the costs;
2. Following in a detailed manner (by means of the 'thin' OBU whereby a great deal of personal data are communicated to the implementing agency) constitutes too drastic an invasion of privacy: the risk of a '(national) tracking system';
3. Personal data can only be made available for commercial purposes with consent obtained in advance. This means that the consent was freely given, relates to a specific form of processing of personal data and that all information necessary for sound decision making is available to the data subject.

d. Administrative consultations between the Ministry of Transport, Public Works and Water Management and the Dutch DPA on 21 April 2008.

The first version of the Kilometre Price legislative proposal and the Kilometre Price Privacy document were presented during the consultations. The draft legislative proposal assumes both a public and a market model.

¹ Recommendations from the *Registratiekamer* of 6 March 2001 (z2001-0336) and Recommendations from the Dutch DPA of 11 December 2001 (z2001-1458)

² Recommendations of 30 March 2006 (z2006-0285)

³ Letters to the Permanent Committee on Transport, Public Works and Water Management of 23 January and 4 February 2008 respectively (z2008-00109)

1. Public Model

In the Public Model, the OBU, which stores travel movements with the aid of GPS information, registers the number of kilometres driven and the relevant rates. Each period (for example a month) the data are sent to a Back Office (BO). The BO subsequently determines the price per kilometre. The BO also searches for the vehicle characteristics (vehicle registration number) that belong to the box. The bill is subsequently drawn up and the invoice is sent to the client.

2. Market Model

The difference with the Public Model is that the aggregation for the purpose of levying the Kilometre Price is performed by a BO that is managed by a private party. A service provider, which shapes the technology, is placed between the government and the motorist. The travel data forwarded are centrally processed in the BO. This system will enable private parties to expand the basic model by offering additional services to the motorist.

II. Assessment Kilometre Price legislative proposal

• Organisational model

The organisation of the collection of the Kilometre Price is based on five pillars:

1. The registration of kilometres driven;
2. The transmission of usage data of the motor vehicle;
3. The calculation of the amount to be paid;
4. The collection of that amount from the owner;
5. Supervision and enforcement.

Page 21 of the EM states the following:

'The Central Government will be responsible for the implementation of the Kilometre Price; it is the Central Government's duty to set the rates in view of the formulated feasibility and environmental objectives and the contributions to the infrastructure fund. Within this context, private service providers will be able, pursuant to this legislative proposal, to take over various implementation activities relating to the Kilometre Price, whereby they will also be able to provide motor vehicle owners with additional services. The Government thus wishes to realise a market with several private service providers.'

This legislative proposal challenges private parties to realise this market, whereby, in time, the entire process will be performed by the market: the so-called end-to-end performance by Multiple Service Providers. The Government has designated this as the Main Process. Because the Government is responsible for timely implementation, work is also underway on a Guarantee Process. The Guarantee Process is a fallback option, which creates a collection agency that is publicly managed. The efforts of the collection agency will be greater or smaller depending on the realisation of the market. It is expected that the market will (for the time being) focus on the first two pillars.

• Registration device (OBU)⁴

All motor vehicles that are subject to the Kilometre Price Act must be equipped with a registration device, which registers the use of a motor vehicle. If an owner uses the services of a private service provider, the services may consist of the supply of this registration device and ensuring that these data are made available, in aggregated form (i.e. all movement data is removed) to the collection agency, which subsequently invoices and collects the amount due.

⁴ This term will be used in the remainder of this document, because the legislative proposal does not speak, or no longer speaks, of an OBU but instead refers to a registration device.

There is also the possibility that the owner acquires all sorts of other services from the private service providers. These could include traffic and route information or a contract for the maintenance of the registration device. If the owner decides against a private service provider, the motor vehicle will have to be equipped with a registration device that directly sends the aggregated usage data to the collection agency (see also EM, pp. 22 and 3, illustrations 2.1 and 2.2).

Page 22 of the EM includes the following in the context of the above:

'The owner of a motor vehicle will be free to decide whether he will make use of the services of private service providers. A possible consequence of choosing a private service provider will be that he makes his personal and movement data available to this service provider. In accordance with the regulations for the protection of personal data, personal and usage data of a motor vehicle can only be used for commercial purposes following explicit consent from the owner. If an owner is unwilling to do so, he must be able to choose direct registration with a collection agency that does not make (commercial) use of such data.'

- **What is registered and how does this take place?**

The registration devices have to be equipped with a GPS receiver and the coordinates of locations where rush hour rates apply. The registration device subsequently maintains a record per type of rate: the distances travelled at certain times and places (movement data). The movement data are only available to the collection agency in aggregated form: collection only requires the data in aggregated form, i.e. the number of registered kilometres travelled against the applicable rates (for example, the rush hour rate).

The registration device will always be equipped with a functionality for supervising the payment obligation. When close to a motor vehicle, supervisors will be able to remotely read the registration equipment, in terms of whether it is turned on, and whether it is functioning properly. Supervision equipment will not be able to read the movement data.

- **Privacy-related aspects**

Paragraph 4.4, Articles 4.17 to 4.20 of the Kilometre Price legislative proposal contain the provisions concerning the protection of personal data. Paragraph 3.4 of the EM (page 31 et seq.) explains these provisions. Article 4.18 of the legislative proposal contains the key provision: who is allowed to process which data pursuant to which regulations. Articles 4.19 and 4.20 of the legislative proposal deal with the retention periods that apply to the Minister and to private service providers respectively.

The legislative proposal assumes two main types of registration system, namely collection through private service providers and the collection agency, and collection performed exclusively by the collection agency⁵. Collection through the private service providers and the collection agency can subsequently be subdivided into service providers that exclusively perform aggregation of movement data for collection purposes and service providers who offer, following consent from the data subject, all sorts of (commercial) services.

The owner of the motor vehicle will be required to choose one of the following options:

- (i) Making use of the collection agency instituted by the Government, which only makes use of aggregated movement data, the aggregation takes place within the registration device ('thick' system, EM, page 23, illustration 2.2);

⁵ See EM, pp. 22 and 23, illustrations 2.1 and 2.2.

- (ii) Making use of the services of a private service provider that aggregates movement data and subsequently sends it to the collection agency ('thin' system, EM, page 22, illustration 2.1);
- (iii) Same as (ii), but on the understanding that, following consent from the owner, the private service provider is allowed to make use of the movement data.

Consent is further elaborated on page 33 of the EM: *'It is important that the owner himself decides whether his movement data can be used and for what purpose. He should grant explicit consent for this purpose to the private service provider and that consent should indicate to what it extends.'*

One of the guarantees is that private service providers will only be allowed to offer services if they have been recognised (Article 4.16 of the legislative proposal). One of the recognition requirements is that the service provider complies with all requirements set by the Wbp. According to the Government, the privacy of the owner is sufficiently guaranteed in each of the above options.

An important decision point for the Kilometre Price is whether the calculation of the payment information should take place locally or centrally:

1. If the calculation takes place locally, in the car within the registration device, the registration device performs the calculation and temporarily stores the results. The registration device downloads the required rate information (place and time zones) from the central Back Office. The calculated payment information is sent to the central back office. This is referred to as the *'thick' registration system* (EM, page 23, illustration 2.2), because the registration device performs the calculation and storage itself.

If a *'thick' registration system* is chosen, this will require a more complex and therefore more expensive registration device. In this case, the central back office will, however, be relatively simple and cheap. The detailed place and time information remains stored in the registration device in the event of a *'thick' registration system* and will therefore not be centrally available. This privacy-sensitive information can, if necessary for example for filing an objection against an invoice, be made available by the motorist to the collection agency. The motorist will, however, remain in control as regards the provision of detailed information. Any checks of the registration device by the competent authorities can remain limited to the aggregated information that can be made available for that purpose by the registration device. All things considered, the system designated as a *'thick' registration system* does not seriously violate privacy.

2. If the calculation takes place centrally in the central back office, the registration device sends all place and time information to the back office. All calculations and storage of data takes place in the central back office. The required rate information (place and time zones) are known in the back office. In this case, the registration device does not do much more than collecting and sending data and is therefore referred to as a *'thin' registration system* (EM, page 22, illustration 2.1).

If a *'thin' registration system* is chosen, this will require a simpler and therefore cheaper registration device. In this case, the central back office will, however, be more complex and more expensive.

The *'thin' registration system* processes privacy-related information centrally; in the

legislative proposal, this therefore takes place at the private service provider. The extent to which privacy is violated depends on the chosen implementation. Generally speaking, there are in the opinion of the Dutch DPA two options:

- a. All place and time information received from the registration device is first stored in the back office and later processed into payment information. This means that every motorist's car movement is stored, in detail, centrally in the back office. It goes without saying that this constitutes a serious violation of the motorist's privacy. The more so because such collection of privacy-sensitive data cannot be properly secured against third parties taking note of them.
- b. All place and time information that is received from the registration device is **directly** processed into payment information in the back office. Only payment information is stored. In this case, the time and place information are only available for a short period of time in the back office. The privacy problem lies in the fact that the motorist must be able to rely on the fact that the back office operator safely processes the time and place information and destroys it immediately after use.

The legislative proposal assumes option a. (see EM, page 22, illustration 2.1). The service provider is only allowed to aggregate the data and to subsequently send it to the collection agency for invoicing purposes, unless the owner has consented to his personal data being used. Movement data may be temporarily stored for this purpose.

An additional privacy problem may arise, in respect of both a *'thick'* and a *'thin' registration system*, if the communications component of the registration device is constantly or regularly engaged. Each engaged telecommunications device can, after all, be continuously traced by the (private) operator of the telecommunications network used by the device. This is a problem that was identified in the case of mobile phones, but also occurs with respect to registration devices, if these start using the same technology. As long as the communications component of the registration devices is engaged, the motorist can be followed by third parties. The legislative proposal does not show whether turning off the registration device is part of the functional requirements of the equipment.

In this connection, the following explanation per article to Article 4.16 (EM, page 90) is interesting: *'The requirements relating to the protection of personal data are particularly important with respect to situations in which the service provider processes movement data received from registration devices. It is, after all, possible, pursuant to Article 4.4(4), to set different functional requirements in respect of the registration devices of clients of service providers. This may concern special categories of personal data, as referred to in Article 16 of the Personal Data Protection Act, which imposes even higher security requirements.'*

This can include, for example, situations in which the owner visits a (psychiatric) hospital or a prison. In order to prevent unauthorised tracking of motor vehicles, the Dutch DPA is of the opinion that a registration device should only occasionally send the aggregated information to the back office, for example once a day. The communications component of the car should be switched off for the rest of the time. If necessary, the communications component of the registration device may be equipped with a so-called *'wake-up'* function in order to comply with control requests from the competent authorities while underway.

It may be interesting for market parties to provide additional services that can be combined with the Kilometre Price system. It would be preferable, from a privacy perspective, not to adjust the aforementioned functionality (by means of the so-called *'wake-up'* function) of the

Kilometre Price system, and the registration device that is part of it. Additional services can best be realised as an optional expansion of the registration system. These extensions to the original service can be supplied as additional hardware and/or software. In principle, extensions can be supplied in such a way that they can be turned off by means of a ‘switch’, for example during weekends (for example, for people driving company cars, see also point III.2 below). If necessary, the extension can make use of additional communication with a private party.

III. Final Assessment

1. A Kilometre Price system utilising a *‘thick’ registration system* will better protect the privacy of a motorist than a system with a *‘thin’ registration system*. A *‘thick’ registration system* is more complex and therefore more expensive, but the associated back office is simpler and cheaper. The Dutch DPA prefers this variant from the perspective of privacy protection; after all, it achieves data minimisation, control of the data remains with the data subject and constitutes a low risk of (undesirable) additional use.
2. If the owner of the motor vehicle chooses a private service provider, the following should be taken into account:
 - If the service provider acts purely as a ‘link’, i.e. it only receives data which it subsequently aggregates for the benefit of the collection agency, such (technical and organisational) measures need to be taken that the service provider will not have access, in any way, to these data for purposes other than those intended here.
 - The consent requirement for using data for other services (Article 4.18(5) of the legislative proposal and page 33 of the EM) requires further elaboration, especially in the EM. The EM should make reference to the concept of consent as referred to in Article 1, at i of the Wbp: *‘consent of the data subject: any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal data relating to them’*.
 - The legislative proposal does not deal with the position of persons driving a company car (there are some 800,000 company cars): to what extent are company car drivers able to choose a *‘thick’ registration system*? In the case of a *‘thin’ registration system*, there should be a possibility of switching off the registration device during private use of the car.
 - In view of the investigation of full performance of the Kilometre Price system by the market (end-to-end), to what extent is it realistic to assume that motorists will still be able to choose a *‘thick’ registration system*? The Dutch DPA considers it necessary that, irrespective of possible end-to-end performance by the market, the motorist will still be able to choose a *‘thick’ registration system*.
3. The market now focuses ‘only’ on the first two pillars of the organisation, i.e. the registration of kilometres driven and sending the usage data to the collection agency. There are, however, currently already investigations underway to have all five pillars performed by the market (so-called ‘end-to-end’ by Multiple Service Providers). This will require an even stricter check from the perspective of the Wbp. The advice of the Dutch DPA will have to be requested if the investigations lead to expansion of the duties of the private service providers and therefore to amendment of the legislative proposal. In other words, the current advice is limited to the performance of the market of the first two pillars.

4. It must not be possible to track the registration device, i.e. it must not be possible to locate the motor vehicle (comparable to a mobile phone). The registration device can be equipped with a ‘wake-up’ function for the purpose of checks by the competent authorities while underway. In the opinion of the Dutch DPA, this requirement should be part of the technical specifications of the registration device.
5. Recognition requirements are set in respect of service providers (Article 4.16 of the legislative proposal). These recognition requirements (financial capacity, reliability, the manner in which the protection of personal data is arranged) are further elaborated in a decree. This decree will, in time, have to be submitted to the Dutch DPA for advice.
6. The Kilometre Price system (the technology, but also the service providers) will be subject to a European tendering procedure, which means that foreign service providers will also be able to make an offer, which in turn could mean that personal data (name, address details and movement data) are processed abroad. The legislative proposal does not deal with these possible consequences.
7. The legislative proposal does not pay sufficient attention to security aspects. What guarantees (both technical and organisational) are there to bring the security of personal data in the back offices but also in the communication traffic between the registration device and the back office to an acceptable level? The Dutch DPA considers it necessary, also in view of the comments below concerning the retention periods, that this is included as one of the recognition requirements set in respect of private service providers, as referred to in Article 4.16 of the legislative proposal.
8. Articles 4.19 and 4.20 of the legislative proposal provide for the retention periods. Article 4.19 of the legislative proposal provides that the Minister will retain the personal data with respect to Kilometre Price due for up to five years following the calendar year in which it became due. This period was derived from the power to as yet proceed with subsequent collection for payment arrears. for up to five years after the claim arose. The Dutch DPA is of the opinion that, in view of the length of this period, it must be further specified which personal data are strictly necessary to be able to as yet proceed with collection. Moreover, measures need to be taken, both organisational and technical, in such a manner that these personal data can only be accessed for this purpose.

Article 4.20, third paragraph, provides for the retention period for personal data held by private service providers. As long as the relevant owner or administrator has not withdrawn his consent, the service provider will be allowed to process personal data for as long as is necessary to perform services or market research or sales activities that are related to the services. The Dutch DPA considers further elaboration necessary in view of the nature of the personal data to be processed. The service provider should at all times, including cases in which consent has been obtained from the data subject, establish whether it is necessary for those purposes to process movement data at the detail level (i.e. data with respect to times, routes, inside or outside of rush hour). Is it necessary, for example, for marketing purposes to process movement data, or can this purpose be achieved by the application of (a certain degree of) aggregation of data?

9. Page 33 of the EM states the following: *“The Kilometre Price Act is not a lex specialis as regards the Personal Data Protection Act, but provides, in some parts, for special regulations with respect to the Personal Data Protection Act. This concerns in particular*

the extension of the Kilometre Price Act to include legal persons.” The Wbp also applies in full to legal person in those cases in which personal data can be traced back to natural persons.

10. The explanation per article to Article 4.4 (EM, page 86) states: *‘This means that the collection agency will not have access to movement data on the motor vehicle and therefore also does not have access to the name and address details of the owner.’* The latter is incorrect, after all, the collection agency will have to send invoices and will need the name and address details of the owner for this purpose.
11. The term ‘movement data’ is lacking in the list of definitions. This term should be included in view of the fact that it concerns a key term.

The Dutch DPA recommends that the Minister of Transport, Public Works and Water Management should *not* submit the Kilometre Price legislative proposal until the abovementioned matters have been taken into account.