COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTAL ADDRESS Postbus 93374, 2509 AJ The Hague VISITING ADDRESS Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Report of findings

Official investigation by the CBP into the processing of geolocation data by TomTom N.V.

PUBLIC VERSION

DATUM 20 december 2011

TABLE OF CONTENTS

1. Introduction

Pursuant to Article 60 of the Wet bescherming persoonsgegevens (Wbp) [Dutch Personal Data Protection Act], the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (Cbp)] has initiated an official investigation into the processing of personal data with regard to TomTom devices made by TomTom N.V. (TomTom).

TomTom collects personal data worldwide via the TomTom devices with the same name, whether mobile or built-in navigation systems, with a screen and built-in GPS sensor with which road users can plan a route. The devices are available in an *offline* and *online* version. In addition the route planner is also available as a smartphone (iPhone) application.

Via the *offline* version TomTom acquires historical geolocation data from users of the devices when they make a connection with their (own) computer to the TomTom servers, for example to install new maps on the devices.

Via the *online* version and the smartphone application, TomTom also offers LIVE services in addition to the route planner such as traffic updates, weather reports, speed camera locations and a facility to search for addresses. Within the framework of the LIVE services TomTom acquires *real-time* geolocation data from users of the *online* devices and the smartphone application. Via the *online* version TomTom also acquires historical geolocation data from users of the devices when they make a connection with their (own) computer to the TomTom servers, for example to install new maps on the devices.

At the end of April 2011 there were media reports to the effect that TomTom supposedly provided geolocation data from users of TomTom devices to third parties, more particularly via the Via.nl traffic advice agency to authorities and the police in the Netherlands, but also directly to commercial parties such as Eindhoven Airport.[1] In response, TomTom sent an e-mail to its users stating that the company wanted to prevent this sort of use of traffic information in the future: *"Yesterday it transpired that the traffic information which we issue is also used by the police to ascertain where motorists often exceed the speed limit and to arrange specific speed checks at those locations. We did not foresee this kind of use and many of our customers are unhappy with this situation. We will therefore include provisions in our licensing conditions to prevent this kind of use in the future"*.[2] The director of TomTom stated in the media that the company had never provided driving data relating to individuals to third parties: *"We have never passed on personal details to the police or any authority whatsoever. The information was bulk information. Averages. Anonymous data."*[3]

[1] "TomTom company discontinues sale of 'speed camera data'", *De Volkskrant*, 28 April 2011, p. 5: "An anonymous spokesperson X [rendered anonymous by the CBP] stated that: 'However TomTom does sell such data directly on to commercial parties. One example is Eindhoven Airport. They use our data to see from which regions their customers mainly come and adapt their marketing accordingly'."

[2] E-mail from TomTom to users, 27 April 2011; see URL: http://uk.support.tomtom.com/cgi-bin/tomtom_uk.cfg/php/enduser/doc_view.php?1=AvVM~wqbfv8QIf5rGhse~yL~Jvsq~5P~EZJBPzr~.

[3] *Algemeen Dagblad*, 28 April 2011, p. 3, "TomTom director also unpleasantly surprised".

The CBP has initiated an investigation in connection with the foregoing on the basis of its supervisory role. The investigation focuses on the following three questions:

- Which data does TomTom process? Is this personal data as defined in Article 1, introduction and under a. of the Wbp?

- Does TomTom have grounds for the processing of personal data as referred to in Article 8 of the Wbp?

- Has TomTom provided personal data to third parties? If so, is this additional processing consistent with the purpose for which the personal data was acquired, as referred to in Article 9 of the Wbp?

The investigation focuses on the assessment of Article 8 (basis for processing: consent, according to TomTom) and Article 9 of the Wbp (compatible with further processing).

2. Course of the investigation

By letter of 28 April 2011 TomTom took the initiative of sending a general clarification to the Minister of Security and Justice, with a copy to the CBP. By letter of 4 May 2011 the CBP requested written information from TomTom. TomTom provided the requested information on 13 May 2011. After studying the information and answers, the CBP obtained oral information from TomTom on 16 June 2011. On 12 August 2011 the CBP again obtained oral information from TomTom.

In its letter dated 6 September 2011 the CBP sent TomTom its report of provisional findings with a request to respond in writing within two weeks. In its letter of 14 September 2011 TomTom requested an additional two weeks to respond to the report of provisional findings. By letter of 23 September 2011 the CBP granted a postponement until 4 October 2011. In a letter dated 3 October 2011, received by the CBP on 30 September 2011,[4] TomTom responded to the report of provisional findings and provided reasoned arguments which parts of the report it believes are company confidential.

Following the response to the report of provisional findings, the CBP obtained new written information from TomTom in a letter dated 3 October 2011. In a letter of 12 October 2011, TomTom asked for the deadline for providing the requested information to be postponed by two weeks. In a letter on 13 October 2011 the CBP granted a postponement until 25 October 2011. TomTom provided the requested information on 25 October 2011.

In a letter on 28 November TomTom provided screen shots and (accompanying) texts to the CBP regarding a proposed new method of providing information and requesting consent. Following consultation by telephone the CBP asked TomTom in a letter dated 1 December 2011 to supply the definitive texts by no later than 8 December 2011. TomTom delivered the newly determined method for providing information and requesting consent on 8 December 2011.

[4] TomTom letter dated 30 September 2011.

In a letter dated 13 December 2011 the CBP sent its report of definitive findings and the draft public version thereof to TomTom with a request to inform the CBP by no later than 23 December 2011 in writing giving reasons whether the draft public version contains company and manufacturing data that are confidential according to TomTom, and if so which parts this concerns. In a letter dated 16 December 2011, TomTom responded to the report of definitive findings and provided reasoned arguments which parts of the report it believes are company confidential.

3. Facts

The object of TomTom, which was established in 1991, with its headquarters in Amsterdam, the Netherlands, is: *"to provide all drivers with the world's best navigation experience"*.[5] TomTom N.V. is established in Amsterdam and has been registered with the Chamber of Commerce since 8 April 2005 under number 34224566.[6] TomTom reported the processing of personal data to the CBP on 27 November 2009 under number 1420031.

TomTom sells mobile or built-in navigation systems with a screen and built-in GPS sensor with which road users can plan a route. These devices have been available in the Netherlands since 2004 in an *offline* version and since 2007 in an *online* version. In addition the route planner is also available as a smartphone (iPhone) application. Using the navigation systems TomTom collects[7] both *real-time* and historical geolocation data worldwide.

Via the *offline* version TomTom acquires historical geolocation data (this means: GPS positions, including accuracy and time) from users of the offline devices when they make a connection with their (own) computer to the TomTom servers, for example to install new maps on the devices.[8]

Via the *online* version and the smartphone application, TomTom also offers LIVE services in addition to the route planner, such as traffic updates, weather reports, speed camera locations and a facility to search for addresses. In that case TomTom acquires *real-time* data, meaning every three minutes the geolocation data collected in the three previous minutes, from users of the *online* devices and the smartphone application. Via the *online* version TomTom also acquires historical geolocation data from users of the *online* version when they make a connection with their (own) computer with the TomTom servers, for example to install new maps on the devices.

The preferred destinations can be set/saved on the devices, such as the users' home location. In addition TomTom collects, on the one hand, the name, sex, e-mail address,

[5] TomTom's mission is, *"To provide all drivers with the world's best navigation experience";* URL: http://corporate.tomtom.com/mission.cfm.
[6] On 13 May 2005 TomTom B.V. became TomTom N.V.
[7] TomTom key facts: *"Our maps cover 104 countries and territories (…)"*; URL: http://corporate.tomtom.com/keyfacts.cfm.
[8] The device can be connected to the TomTom servers via the built-in USB port or by removing the SD memory card using the TomTom HOME software application. TomTom HOME is referred to as MyTomTom on devices manufactured after October 2010. TomTom information 13 May 2011, Annex 1, p. 4.

country (choice), address and telephone number and, on the other hand, the account name and serial numbers of the devices of users who register online and who purchase devices via the TomTom web shop.[9] In addition TomTom collects, on the one hand, the name, sex, e-mail address, and country (choice) and, on the other hand, the account name and serial number of the devices of users who register online and who purchase application subscriptions via the software.[10] Lastly TomTom collects serial numbers and other identifying data from users in the case of (some) promotions and/or exchange promotions[11] and also repairs [12] and name, e-mail address, address, telephone number, serial number, purchase date and information about a support or service issue in the event of, for example, technical support (customer service for products and/or services).[13]

TomTom declares that all processing of "travel time information" is based on consent.[14]

3.1 Offline data processing: historical geolocation data

TomTom devices, both the *online* and the *offline* versions, have a standard (factory) setting whereby they do not save any geolocation data. The devices only record geolocation data after the user has selected "Yes" in reply to a question for consent to collect data. This question is displayed on the device after a number of user hours.[15] The question text reads as follows:

"TomTom would like to collect a number of non-personal details to improve our products. The details (for example on the actual journey time via certain roads) are collected each time you connect your TomTom navigation system to your computer. This has no effect on the speed of your internet connection and costs you nothing. All the details collected are anonymous. Do you give us consent to collect these details? No Yes."[16]

If the user chooses "No", but connects the device later via an (own) computer to the TomTom servers, the user will be asked a similar question via the software application. This question reads:

"TomTom wants to collect anonymous statistical data to improve the map quality and your navigation experience. The idea is that we repeatedly retrieve this data when your TomTom navigation system connects with the TomTom server. You will not notice anything and this

[9] This concerns a small percentage of sales of devices. TomTom information
25 October 2011, p. 3.
[10] Ditto, p. 3-4.
[11] Ditto, p. 4.
[12] Ditto, p. 5.
[13] Ditto, p. 4-5.
[14] TomTom letter to the Ministry of Security and Justice and the CBP on 28 April 2011, p. 2: "We ask our customers for consentconsent to collect travel time information. They can provide this consent and also withdraw it"; TomTom information 13 May 2011, p. 1: "We have always informed customers in three ways and asked consent regarding the fact that we want to collect travel time information."
[15] TomTom information 13 May 2011, Annex 1, p. 6.
[16] Ditto, see Annex 8.

costs you nothing. If you set this preference, we will be able to collect this data. <link to website> TomTom Privacy Policy".[17]

If the user again chooses "No", TomTom will not collect any geolocation data.[18]

If the user chooses "Yes" (the first or the second time), the device will create an empty file which will be used to store data on the use of the device from that moment. On the one hand this is data about turning the device on and off and data about the device model and, on the other hand, detailed data on routes travelled by the user. Using the built-in GPS-sensor, the device saves its exact position in this file, including the accuracy and time. This is done very frequently.[19] The file does not contain a unique number, such as a serial number or an account name. Nor is the file name unique; rather it is identical on each device.[20]

In response to the report of provisional findings, TomTom announced that it was going to expand and specify the consent request and accompanying information for the *offline* and *online* devices (see paragraph 3.2).

From a technical point of view (a maximum of) four successive data processing activities take place after the user has selected "Yes".

Firstly the geolocation data is stored in encrypted form on the device. The data continues to be stored on the device until the user connects the device via an (own) computer to the TomTom servers.[21]

Second, TomTom receives the file with the historical geolocation data and the IP address of the Internet connection (of the user). If the user opts to connect the device to the TomTom servers, for example to download/install new maps on the device, the device automatically sends the file with the historical data on routes driven by the user to the TomTom servers.[22]

In response to the report of provisional findings, TomTom provided additional information about the sending of the file: the file is received by TomTom on an incoming *reverse* web proxy. The encrypted file is captured in its entirety in this web proxy.[23] The file with historical geolocation data is forwarded within several tenths of a second to the protected internal TomTom network. After this transfer the file is irrevocably deleted from the non-persistent working memory of the web proxy. The IP address of the internet connection (of the user) is then replaced by the internal IP address of the web proxy.[24]

[17] Dutch (instead of English) text supplied in response to the report of provisional findings. TomTom letter dated 30 September 2011, Annex 5, p. 12.

[18] TomTom information 13 May 2011, p.1-2.

[19] The frequency depends on the software version and the device model. Ditto, Annex 1, p. 6.

[20] Ditto.

[21] TomTom letter dated 30 September 2011, Annex 1, p. 6.

[22] Ditto.

[23] Ditto, p. 4.

[24] Ditto, p. 4 and 6.

TomTom declares that it does not collect any additional data via the file with geolocation data, such as an account name (chosen by the user):

"For the sake of clarity let it be stated that other communication flows, whether accompanied by an account name or device serial number, from the TomTom HOME application, take place entirely independently of and to separate servers based on an irregular pattern which is unpredictable as regards time."[25]

The file with historical geolocation data does not contain any unique numbers or other identifying characteristics of (the user of) the device, except for that data which, because of its uniqueness, can be directly or indirectly traced to an individual user (for example because a route has been driven at a deviating time in a thinly populated area).

The existing data on the device is automatically deleted after the transfer of the historical geolocation data to the TomTom servers. A new empty file is created on the device.[26]

Third, TomTom processes the data by decrypting the individual trips from the rough file (which can cover a period of months or even years [27]).[28]

Fourth, TomTom stores the data of the various trips in general archive servers.[29]

The last two processes take place in *real time*, in non-persistent memory (in other words: no data is stored to a file on the hard disk).

3.2 Online data processing: real-time geolocation data

The purchase of new *online* devices includes as standard 1 year's subscription to the LIVE services,[30] of which the HD Traffic (traffic information) service is part. LIVE services are automatically activated when the device is turned on.[31] In the case of the smartphone application, the paid HD Traffic service is purchased within the application, in addition to the route planner.

For the purposes of the HD Traffic service, the *online* devices and the smartphone application with the HD Traffic subscription make automatic contact with the TomTom servers as soon as they are switched on. The mobile internet connection and the built-in SIM card for the *online* devices are supplied in the Netherlands by one of

[25] Ditto, p. 5.
[26] Ditto, p. 6.
[27] In response to the report of provisional findings TomTom added that "*devices with this functionality have only been used since the end of 2007*" and that *"devices are limited in their storage capacity, which leads to collection on the device being stopped well before any risk of exceeding* [the limit]." Ditto, Annex 5, p. 12.
[28] Ditto, Annex 1, p. 6.
[29] Ditto.
[30] Until 2010 a period of 3 months was included as standard. There is an initial trial subscription of 3 months for devices which are permanently built into cars. TomTom oral information 12 August 2011 and TomTom letter 30 September 2011, Annex 5, p. 12.
[31] Except in the case of devices which are permanently built into cars. TomTom letter dated 30 September 2011, Annex 5, p. 12.

the network operators with which TomTom has a contract. In the case of the iPhone the (kind of) internet connection depends on the user.

The locations are sent in combination with the unique serial number of the device, and the account name.

The general TomTom privacy statement contains the following information about the processing of geolocation data with regard to the HD Traffic service:

"If You subscribe to TomTom location-based services like HD Traffic, TomTom may collect location data from Your TomTom device in order to provide You with the services requested."[32]

In addition the TomTom privacy statement contains the following general information on the processing of geolocation data: *"TomTom may gather Anonymous Information from Your TomTom device when You are using it or when You are connecting it to a computer by using TomTom HOME. This Anonymous Information includes location information (information about Your location), information on how long it took You to travel certain routes, traffic patterns and on any technical glitches You may have encountered. The nature of the Anonymous Information that Your TomTom device transmits to us will not enable us to trace it back to an identifiable person; provided, however, You may elect to permit us to associate such Anonymous Information with Personal Information we have collected from You to provide You with specific location-based services that are tailored to meet Your needs or interests, to improve our products and services or to enforce the agreements, terms and conditions related to our Websites, products and service."*[33]

In the information obtained orally on 12 August 2011, TomTom declared that users are not asked individually for consent for the processing of data in relation to this LIVE service.[34]

Within the smartphone application the following purchase information is provided on the specific HD Traffic service:

"As part of the TomTom HD Traffic service, location data is sent to TomTom, which is then used anonymously to improve the quality of the traffic information for all our subscribers. By purchasing this product you agree to share this data with TomTom."[35]

In the written information TomTom indicates that it, during the course of 2011, *"foresees a standardisation and improvement of the phrasing used, explanation and clarity of the consent. We will implement this in phases for our entire product range."*[36] The information includes an annex with the draft new method of informing and obtaining consent for "the collection and transfer of information to TomTom" which will first be implemented in new built-in *online* devices.[37]

In response to the report of provisional findings TomTom declares:

[32] Annex 2 to TomTom letter to the Ministry of Security and Justice and the CBP of 28 April 2011

[33] Ditto.

[34] See also TomTom letter of 30 September 2011, Annex 5, p. 13.

[35] TomTom information 13 May 2011, Annex 10.

[36] Ditto, p. 2.

[37] Ditto, see Annex 13.

"We will certainly make new software available in January 2012 for the navigation products which we supply to consumers and have supplied to consumers in the past. This automatic update contains a more detailed explanation and explicit questions for the processing of geolocation data. We will also adapt our website and our public privacy policy with regard to these points. In addition we will involve the processes which are not subject to the WBP."[38]

TomTom also states that the consent request prior to the processing has since been included in the new *online* devices that are to be built in.[39]

By letter of 8 December 2011 TomTom states that the new method of informing and asking consent will be implemented in the second half of February 2012, in a software update for all *offline* and *online* devices and the smartphone application.[40]

According to screen shots and the texts which TomTom provided to the CBP on 28 November and 8 December 2011, consent will be requested in/from this software update for the *offline* and *online* devices as follows:[41]

"We would like to collect some information about your use of this navigation device. The information is stored on this device until we retrieve it. We use it anonymously to improve our products and services.[42]

Will you help us and allow this?

"No/More Info/Yes"

If the user chooses "More info", he will see the following text:[43]

"Only if you give us your permission, your navigation device will continuously collect information. The information is stored on your device until you connect it to your PC, then the information is sent to TomTom and deleted from your device. The information includes details that identify the navigation device, details about routes and locations and information entered while you were using the navigation device.

Immediately after receiving this information, TomTom automatically and irreversibly destroys any data that allows identification of you or your device. This, now anonymous, information is

[38] TomTom letter dated 30 September 2011, p. 1.

[39] Ditto, Annex 4, p. 11.

[40] TomTom letter dated 8 December 2011, p. 1. TomTom states that it encountered delays when formulating this software version [CONFIDENTIAL].

[41] TomTom has provided texts in English to the CBP. For Dutch users these texts will become available in Dutch, but the translation was not yet ready and approved by TomTom at the time of this investigation.

[42] The consent request for the *online* devices is a little more extensive, and also contains the following sentence: *"If you use LIVE services, we will also use your location information to deliver the services to you."*

[43] The text for the *online* devices differs or is a little more extensive than the text quoted above, and contains, amongst others, the following elucidation, in the middle and at the end of it: *"Within twenty minutes of switching off your navigation device, TomTom automatically and irreversibly destroys any data that allows identification of you or your service (…)."* En: *"If you no longer allow sharing of information (…) You won't be able to receive HD Traffic or mobile speed camera locations, or use any other LIVE services*." Further more the text for the *online* devices states that TomTom also collects the MyTomTom accountname in all cases.

used to improve TomTom's products and services, such as maps, reports on Points of Interest and average speeds driven. These products and services are also used by government agencies and businesses.

Using your navigation device, you can join the MapShare Community or report speed cameras[44]*. If you choose to use either of these services, your reports, that include location information and your MyTomTom account name, are sent to TomTom and kept together with your MyTomTom account. TomTom then uses your information to improve its maps and speed cameras.*

If you no longer allow sharing of information, none of the above information is sent to TomTom and information previously stored on your device is deleted.
TomTom will not give anyone else access to the information collected from your navigation device.

In choosing to provide TomTom with information you are helping to make driving better, specifically by improving maps, traffic flows and reducing congestion. We appreciate your help. If you think that your information is not being used for the purpose for which you have provided it to TomTom, contact us at http://tomtom.com/support.

See our privacy policy at http://tomtom.com/privacy."

It is possible to withdraw consent for both sorts of devices at any time by revisiting the options screen and by selecting "No".[45] After consent has been withdrawn, the file with historical location data will be deleted. TomTom states the following on this:

"In addition to this, it is the case that if you select "no", information already collected on the device for transfer is deleted so that, if a connection is made to the PC, there will be no (historical) data which can be transferred, including from before the time that permission was withdrawn."[46]

As regards the smartphone application[47] TomTom states that, as from the software update in the second half of February 2012, consent will be requested in the following manner:

"Data Sharing

Some features of this application need to collect and send information about you and your device to TomTom and others you explicitly select. TomTom also uses this information anonymously to improve its products and services. Below you can find more details of the information that is shared by each feature, how this information is used and how you can stop sharing information.

[44] The services MapShare Community and reporting speed camerashave not been investigated by the CBP.
[45] TomTom states: "Withdrawing and giving consent again are possible at any time via the 'Settings menu' by choosing the 'Me and my device' option there. You can then select 'My information' in this submenu." TomTom letter dated 28 November 2011, p. 4.
[46] Ditto, p. 6.
[47] [CONFIDENTIAL].

Will you help us and allow this?

<Yes> <No>"[48]

The text of the accompanying information (explanation) reads as follows:

"General

In order to perform its intended function, this navigation App fundamentally requires location information from your device. Some features of this App require sharing of this location information via the device's internet connection with TomTom or others you explicitly select. In those cases information identifying you or your device is also shared. This is required to be able to send the requested information back to your device, to verify your subscription status, to help improve the service quality or because sharing information about your whereabouts is what you intend.

In those cases where TomTom receives and uses location information, TomTom never keeps a stored record of your location while you are using the App. Within 20 minutes of closing the App, TomTom automatically and irreversibly destroys any data identifying you or your device. (…)

In choosing to provide TomTom with information you are helping to make driving better, specifically by improving maps, traffic flows and reducing congestion. We appreciate your help. (…)

You can disable and enable information sharing at any time using the "data sharing" switch in the settings menu. (…)"

The explanation also includes information which can be used per service, such as HD Traffic, Google search, [CONFIDENTIAL].[49]

TomTom also states the following in this connection: "*Data sharing has to be switched to 'on' for all services. If this is not the case, no data is exchanged and the user is notified to this effect and referred to the settings menu for more information and to switch on data exchange."*[50]

TomTom states that the majority of users in the Netherlands use the software update within two to three months, including for the *offline* devices.[51] TomTom writes: *"In addition to updating the software the update is initially intended to update maps, MapShare updates, permanent speed cameras, the installation of purchased voices or the user's own collection of Points of Interest/Useful Locations. TomTom actively encourages users in various ways to keep their device up-to-date by regularly connecting it to their PC or Mac. This encouragement takes the form of the e-mail newsletter, messages/tips which occasionally appear on the device itself and, for the new generation of devices, by means of updates being reported on the PC/Mac, even if the device is not connected. (…) For new devices it is the case that users*

[48] Letter TomTom of 8 December 2011, Annex 4, p. 1.

[49] Ditto.

[50] Ditto, Annex 3, p. 1.

[51] TomTom letter dated 8 December 2011, p. 2.

are encouraged to connect their device shortly after purchasing it, to download the latest version of the map and software free of charge. (…) On the basis of experience with previous software updates it can be stated that new software versions have been properly distributed within 2 to 3 months."[52] This period also applies to the iPhone application, according to TomTom.[53]

From a technical point of view, six data processes take place in the case of the *online* devices and the smartphone application (in addition to the above-mentioned four *offline* data processing operations[54]).

First and foremost, after the user has turned on the *online* device or the smartphone application, TomTom collects the serial number and account name for the purpose of access verification.[55]

Second, the device automatically collects geolocation data from the user and encrypts this.[56]

Third, the device sends the (encrypted) geolocation data that has been stored in the meanwhile every three minutes to the TomTom servers.[57]

Fourth, there is an intermediate phase before the (encrypted) data is transferred to the archive servers. This involves the serial number being replaced by a new unique number, referred to as the BUID. The link between the serial number and the unique new number is broken after a maximum of 24 hours because the serial number is deleted.[58]

In addition to the report of provisional findings, TomTom states that this period of a maximum of 24 hours has been reduced since 27 April 2011, and that the link between serial numbers and the BUID is automatically deleted at the latest within 20 minutes after the device has been switched off.[59]

Fifth, TomTom combines the above-mentioned data[60] in another system with data from various data sources (including traffic jam information from the Dutch Traffic Centre (Verkeerscentrum Nederland) and travel details from mobile telephones via operators).[61]

[52] Ditto.

[53] Ditto.

[54] This means: as far as the *online* devices are concerned.

[55] TomTom letter dated 30 September 2011, Annex 3, p. 10.

[56] Ditto. In response to the report of definitive findings TomTom has indicated that this phase (that is: the interim storage of the (encrypted) geolocation data) also takes place in the non-persistent memory. This does not prejudice the fact that simultaneous storage of geolocation data in the permanent memory takes place for the purposes of the file with the historical geolocation data. TomTom letter dated 16 December 2011, p. 3.

[57] Ditto.

[58] Ditto.

[59] Ditto, Annex 3, p. 8.

[60] The individual uploads can be related to each other via the BUID. TomTom information 13 May 2011, Annex 1, p. 9.

[61] Ditto, p. 10.

Sixth, the geolocation data is saved every 24 hours to archive servers (historical journey archive). The BUID is then deleted. The data on these archive servers do not contain any unique numbers or other identifying features of (the user of) the *online* device or the smartphone application, apart from that data which, because of their uniqueness, can be directly or indirectly traced to an individual user (for example because a journey has been completed on a less busy deviating point in time in a thinly populated area).

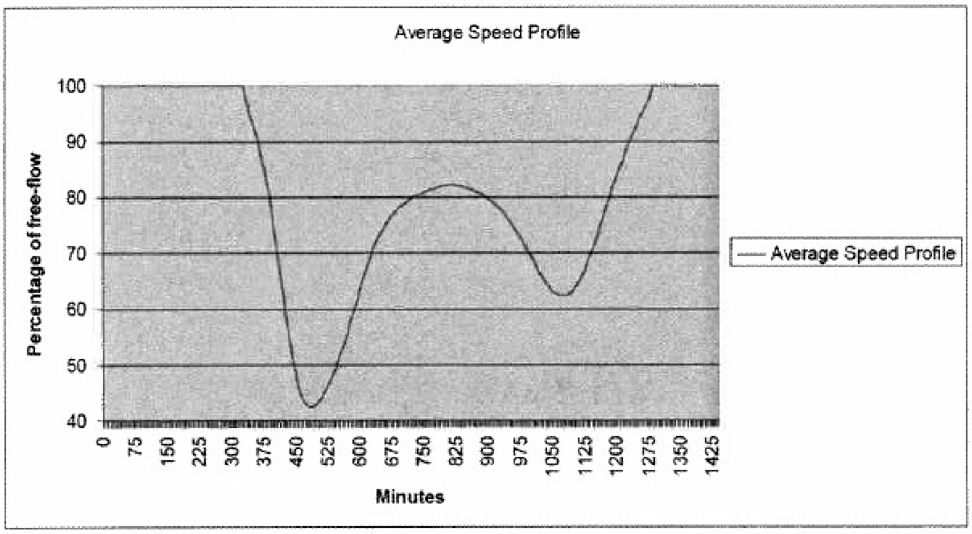
[CONFIDENTIAL][62]

From the first phase onwards the processing takes place in *real time*, in non-persistent memory. This means: no data is stored in a file on the hard disk.[63]

3.3 Additional information

TomTom provides journey details from the archive servers (which contain data from both the *offline* and the *online* devices and the smartphone application) at an aggregated level to third parties. TomTom refers to four forms of aggregation: historical file information, occupancy rate of road sections, "speed profiles" and [CONFIDENTIAL].

A *speed profile* means that, according to the direction of travel per time of the day of the week, an indication of the driving speed is given per road segment. Road segments can vary in length, from a couple of metres to tens of kilometres.[64] An example of a speed profile[65] is:



[62] [CONFIDENTIAL]

[63] Ditto, p. 7 and the additional statement in the oral information on 16 June 2011.

[64] A road segment is a connecting segment between two road junctions, as for example in crossing or transition between different kinds of roads.

[65] Annex 1 with TomTom letter to the Ministry of
Security and Justice and the CBP of 28 april 2011.

[CONFIDENTIAL]

TomTom declares that it has never fully or partially provided the data from the different systems (databases) in rough (non-aggregated) form to third parties.[66] TomTom has provided the aggregated data from the archive servers in return for payment directly or indirectly to third parties, such as local and provincial authorities [67], Eindhoven Airport[68] and a traffic advice bureau. This traffic advice bureau (Via.nl) has provided the aggregated data to law enforcement authorities, sometimes for payment.

In a fact sheet on the speed profiles obtained from TomTom the traffic advice bureau Via.nl stated:

"The Speed Profiles database contains information about the speed driven:

- *per stretch of road/road section*
- *the direction of travel*
- *per day of the week*
- *average per 15 minutes*

For each separate stretch of road it is then known per direction of travel how fast, on average, traffic has driven during the day. (…) Of all the measurements, the lowest and the highest speeds (the extremes) are not included in the calculation of the average".[69]

TomTom states that it itself continues to process aggregated journey data from the archive servers to improve map material, for example to indicate that a crossroads has become a roundabout.[70]

4. Assessment

4.1 Controller

On the grounds of Article 1, introduction and under d, of the Wbp the controller is *the natural person, legal entity or any other administrative body that, alone or together with others, determines the purpose of and the means for the processing of personal data*.

TomTom, established in Amsterdam, the Netherlands sets the purposes of and the means for the processing of personal data with regard to TomTom devices. TomTom is therefore responsible within the meaning of Article 1, introduction and under d. of the Wbp for the processing of personal data with regard to TomTom devices.

[66] TomTom information 13 May 2011, Annex 1, p. 8: "The data is and has never been made available entirely or partially 'as=is' or in rough form to third parties, in order to prevent possible de-anonymisation. [CONFIDENTIAL]"

[67] TomTom letter to the Ministry of Security and Justice and the CBP of 28 April 2011, p. 2: "We also make this travel time information available to local and provincial authorities. This enables them to see how and where traffic jams occur and to take specific measures to improve traffic flows and make our roads safer."

[68] See footnote 1.

[69] Via.nl, Speed Profiles Fact sheet, 31 March 2011. URL: http://www.via-advies.nl/download/pdf/NL_Factsheet%20Speed%20Profiles.pdf.

[70] TomTom information 13 May 2011, Annex 1, p. 8.

4.2 Processing of personal data

According to Article 1, introduction and under a. of the Wbp personal data means: *any data concerning an identified or identifiable natural person.*

"Processing" of personal data is defined in Article 1, introduction and under b. of the Wbp and includes, among other things, the collection, [71] recording and storing of personal data.[72]

Information "concerning" a natural person
Data that partly determines the way in which the data subject is assessed or treated in society is personal data.[73] The use that is made of the data therefore partly determines the answer to the question whether the data is personal data.[74] Data which is not directly related to a certain person but, for example, to a product or a process, may provide information about a certain person and is in that case personal data.[75] *Identifiability of the person*A person is identifiable if his identity can reasonably be determined either directly or via additional steps,[76] without disproportionate effort.[77] Identification can also take place without the name of the person involved being discovered.[78] In order to determine whether a person is identifiable, an assessment has to be made of all resources which one can assume can reasonably be used by the controller or another person to identify the person (objectified assessment).[79] It is necessary to assume that the controller is reasonably equipped. [80] In concrete cases, however, account has to be taken of special expertise, technical facilities, and the like of the controller.[81] Only if tracing the data to a person requires a *disproportionate effort* on the part of the controller is the data not regarded as personal data.

TomTom processes - in various systems - the following combinations of data: the unique serial numbers of each device with secondary data on the device, TomTom account details (account name, name, sex, e-mail address, and country (choice)) sometimes with the address and telephone number, precise geolocation data on the basis of GPS satellite measurements, travel details (from which driving speed can be derived) and the IP address of the internet connection (of the user).

Concerning the geolocation and travel details TomTom declared:

[71] Collection already is involved if the data is acquired and then immediately destroyed. Parliamentary documents II 1997/98, 25 892 no. 3, p. 68.
[72] Article 1, under b, of the Wbp interprets – verbatim – "processing of personal data" as: "*any action or set of actions with regard to personal data, including in any event the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data."*
[73] Parliamentary documents II 1997/98, 25 892 no. 3, p. 46.
[74] Ditto.
[75] Ditto.
[76] Parliamentary documents II 1997/98, 25 892 no. 3, p. 48.
[77] Ditto.
[78] WP29 136, Advice 4/2007 on the term personal data, 20 June 2007. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf.
[79] Parliamentary documents II 1997/98, 25 892 no. 3, p. 48.
[80] Ditto, p. 48-49.
[81] Ditto, p. 49.

"It should be stated beforehand that TomTom treats each item of data that is sent from a TomTom navigation system to TomTom as an item of personal data within the meaning of the Wbp."[82]

In response to the report of provisional findings, TomTom conversely declares that it is of the opinion that the processing of historical geolocation data is not the processing of personal data:

"TomTom has made substantial investments and efforts to ensure that, where persons might be identifiable, this may not be possible in practice, by the very extensive application of Privacy Enhancing Technologies and Privacy-by-Design, and also by the organisational structure of the processing. This guarantees that identifiable data together with geolocation data are never actually accessible in the processing chain in either "space" or "time", nor can they be made accessible or constructed later.

TomTom did this precisely because it realised in 2007 that geolocation data can give an intrusive insight into someone's (road) behaviour. TomTom is of the opinion that the acquisition of that behavioural image can best be prevented by not linking any identifying characteristics to the geolocation data or, in instances where this is impossible, by ensuring that the link is always so short-term and so well protected through use of technical and organisational means, that the construction of a behavioural image or other forms of identifiability cannot actually be achieved in practice, either at the time of the processing or after processing has ended.

TomTom is of the opinion that it has fully succeeded in this as regards the processing of offline geolocation data.

TomTom therefore takes the view that the processing of offline historical geolocation data which it has set up is not processing of personal data in the sense of the WBP, or, in so far as this concerns IP addresses, this can take place on the basis of one of the other grounds ("performance of contract", WBP Art. 8b or "legitimate interest" WBP Art. 8f."[83]

TomTom states the same in this response with regard to the processing of *real time* geolocation data.[84]

After this, an assessment is provided per processing as to whether personal data is being processed.

4.2.1 Historical geolocation data

With regard to historical geolocation data, in the case of <u>*offline* and *online* devices</u>, personal data is processed in two processes, in effect different phases of the processing by TomTom. *In the first instance when the geolocation data* ***is stored on the device****. In the second place when* ***TomTom sends and receives*** *geolocation data.*

[82] TomTom information 13 May 2011, Annex 1, p. 3.
[83] TomTom letter dated 30 September 2011, Annex 2, p. 7.
[84] Ditto, Annex 4, p. 11.

Geolocation data stored on the device itself: identification by a third party or TomTom
On the basis of the routes travelled in combination with the exact GPS location data (including accuracy and time) it can be deduced where someone (the data subject) apparently lives and works and whether someone was, for example, present at a crime scene.[85]

Such information (from a confiscated device), whether or not combined with data from the (national) vehicle registration system and/or historical data from a mobile telephone, is regularly used by the police in practice for law enforcement purposes.[86] The police are able to retrieve the name of the data subject, for example via the vehicle registration system, and link the historical geolocation data to the user.

If they can access the TomTom device, third parties and TomTom itself may be able, for example, to identify the individual user via the last selected route or the set/stored home location (street and house number), whether combined or not with the name on a name plate. There are no passwords on the devices. [87]

TomTom can decipher individual routes from the rough, encrypted file.[88]

Every TomTom device has a serial number.[89] In one or more of the following cases, TomTom holds files in which the serial numbers together with other identifying data of the data subject (such as the name, e-mail address, etc.) are recorded:

1. The device was purchased via the TomTom webshop.
2. The purchaser used a TomTom discount or exchange promotion.
3. The user contacted the customer services and/or technical support.
4. The user has created a MyTomTom account via MyTomTom/TomTom HOME which is linked to the device.[90]

As a result TomTom itself also has the means to identify individual users of devices.

TomTom is also able to couple historical geolocation data to the individual user if this user has himself contacted TomTom with a question or request for technical support for his device and has made the device available to TomTom.

It is not relevant whether TomTom intended to use the geolocation data for law enforcement, marketing or profiling purposes. Data already are personal data if the

[85] In other words: information “concerning” a natural person.

[86] District Court of Zutphen 25 February 2011, *LJN* BP5729. See also District Court of Haarlem 3 November 2010, *LJN* BO2789 and District Court of Zwolle 6 May 2010, *LJN* BM3601. See also Definitive findings of the CBP Investigation into the collection of Wifi data with Street View cars by Google dated 7 December 2010, p. 35 (z2010-00582). URL: http://www.cbpweb.nl/Pages/pv_20110913_google.aspx.

[87] Only older generation devices offer the possibility, after the user has created an account, to set a 4-figure pin code via TomTom HOME. TomTom letter dated 16 December 2011, p. 3.

[88] See footnote 28.

[89] As regards the *offline* devices the geolocation data is saved in a file without additional data such as a serial number or account name.

[90] TomTom information 25 October 2011, p. 5.

data can be used for such a purpose that focuses on the person, and that possibility *de facto* exists.[91] The legislative history of the Wbp contains the following remarks:

"Contrary to what the Registration Board states in its recommendation, it is not required that all possibilities to use data related to persons are excluded. If this is a theoretical possibility, but it is inconceivable that it will actually happen, it may be assumed that the data are not regarded as personal data. If it is possible, however, to use the data to investigate fraud, these data will be regarded as personal data. Whether or not there is an intention to use the data for this purpose is not relevant. Data are deemed personal if they can be used for such person-oriented purposes" (underlining by CBP).[92]

In response to the report of the provisional findings TomTom states that *"in all cases(…) the other identifying data* [is] (added by CBP) *kept completely separate from the processing of geolocation data (both offline and online) and these processes are arranged in such a way that identifiability via the serial numbers is excluded by the technical and organisational measures which TomTom has taken."*[93]

The fact that the data is stored on the device in encrypted fashion and that the other identifying data is, in principle, kept separate from the geolocation data, does not lead to the conclusion that the data is not personal data. In view of its technical (decryption) possibilities and the current computation power of computers, TomTom must be considered capable of decrypting the file with geolocation data – without disproportionate effort – and of linking it to other identifying data of the data subject (such as name, e-mail address, etc.).[94]

However, the fact that identification-limiting measures have been taken will play a positive role in the context of an assessment of whether the security obligation in Article 13 of the Wbp has been fulfilled.[95]

Geolocation data sent from the device and received by TomTom: identification by TomTom

TomTom states that – besides the IP address of the internet connection (of the user) – it does not collect any additional data with the file with geolocation data, such as an account name (chosen by the user himself).[96] The file with historical geolocation data does not contain any unique numbers or other identifying characteristics of (the user of) the device, except that data which, because of its uniqueness can be directly or indirectly traced to an individual user (for example because a route has been driven at a deviating time in a thinly populated area).

Identification can also take place without the name of the data subject being discovered.[97] The only requirement is that the data subject can be distinguished from

[91] In a criminal case at the District Court of Zutphen it transpired that the police had examined the last *point of interest* entered and the *Last Journey Information* list. District Court of Zutphen 25 February 2011, *LJN* BP5729.

[92] Parliamentary documents II 1997/98, 25 892 no. 3, p. 47.

[93] TomTom information 25 October 2011, p. 5.

[94] See footnote 86.

[95] The CBP has limited this investigation to compliance with the provisions of Articles 8 and 9 of the Wbp.

[96] TomTom information 25 October 2011, p. 5.

[97] See footnote 78.

other people by means of the available information in combination with other data (whether the latter is retained by the data controller or not).[98]

The opinion on the term personal data of the joint European supervisory bodies as regards the protection of personal data states the following:

"(…) that, while identification through the name is the most common occurrence in practice, a name may itself not be necessary in all cases to identify an individual. This may happen when other "identifiers" are used to single someone out. Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data also reflects this fact."[99]

It is therefore important whether the data subject can be "individualised".

The file with historical geolocation data contains detailed information about routes driven in combination with the precise GPS location data (including accuracy and time). This data provides a first-hand insight into someone's behaviour. This can, for example, be used to find out where someone (the data subject) apparently lives and works and when someone goes on a journey. The data subject can therefore be "individualised".

In addition, TomTom is also actually able to find out [100] the name of the data subject. TomTom can link the data to the person or the user via (i) his IP address and (ii) his assumed home and work address (via log options on the web proxy).[101]

After the file with historical geolocation data has been forwarded to the protected internal TomTom network, the file has been irrevocably deleted from the non-persistent working memory of the web proxy, and the IP address of the internet connection (of the user) has been replaced by the internal IP address of the web proxy, TomTom will have irrevocably removed all features from the data that could directly or indirectly identify the individual data subject. Neither TomTom nor anyone else

[98] WP29 136, Advice 4/2007 on the term personal data, 20 June 2007. URL: 14. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf. *"In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others."*

[99] Ditto, p. 14 and 15.

[100] This means: the avoidance of technical and organisational measures does not require a disproportionate effort, given TomTom's technical (decryption) options and the computation power of modern computers.

[101] (Until) the moment that the file is received on the incoming *reverse* web proxy.

can then, in principle, directly or indirectly trace the data back to the individual data subjects without disproportionate effort.[102]

4.2.2 *Real-time* geolocation data

If the data is *real-time* geolocation data, in the case of *online* devices and the smartphone application, the personal data is processed in the first data processing phase by TomTom.

In this first phase TomTom also automatically receives, when collecting the *real-time* geolocation data, the unique serial number of the device and the account name of the data subject. TomTom can use the combination of data on routes travelled by the data subject[103] and, for example, the account details or the serial number of the device to trace an identifiable natural person.

TomTom records the account name, name, sex, e-mail address and (choice of) country. In addition, in one or more of the following cases, TomTom has files in which the serial number together with other identifying data of the data subject (such as the name, e-mail address, etc.) are recorded:

1. The device was purchased via the TomTom webshop.
2. The purchaser used a TomTom discount or exchange promotion.
3. The user contacted the customer services and/or technical support.
4. The user has created a MyTomTom account via MyTomTom/TomTom HOME which is linked to the device.[104]

In response to the report of the provisional findings, TomTom states that *"in all cases (…) the other identifying data* [is] (added by CBP) *kept completely separate from the processing of geolocation data (both offline and online) and these processes are arranged in such a way that identifiability via the serial numbers is excluded by the technical and organisational measures which TomTom has taken."*[105]

The fact that the other identifying data is kept separate by technical and organisational measures from the geolocation data, does not lead to the conclusion that the data is not personal data. In view of its technical (decryption) possibilities and the current computation power of computers, TomTom must be considered capable of decrypting the file with geolocation data – without disproportionate effort – and of linking it to other identifying data of the data subject (such as name, e-mail address, etc.).[106]

What is more, identification can also take place without the name of the data subject being discovered.[107] The *real-time* geolocation data contains detailed information about routes driven in combination with the precise GPS location data (including accuracy and time). This data provides an intimate overview of someone's behaviour. This can,

[102] This applies except where the segmented data on routes driven is directly or indirectly traceable back to an individual user (for example because a route has been travelled at a less busy, deviating time in a thinly populated area).
[103] See footnote 86.
[104] TomTom information 25 October 2011, p. 5.
[105] Ditto.
[106] See footnote 91.
[107] See footnote 78.

for example, be used to find out where someone (the data subject) apparently lives and works and when someone goes on a journey. The data subject can therefore be "individualised".

However, the fact that identification-limiting measures have been taken will play a positive role in the context of an assessment of whether the security obligation in Article 13 of the Wbp has been fulfilled.[108]

In the second phase TomTom replaces the serial number with a new temporary unique identifying number (BUID). For a maximum period of 24 hours[109] a link is available in non-persistent memory (random access memory) between the serial number and the new temporary number. During the time that this link is possible, TomTom cannot however - as has become apparent - discover the movements of individually identifiable data subjects without disproportionate effort (for example: special additional equipment/software). This has to do, for example, with (i) the transience of the table which links the serial numbers to the BUID: the link is deleted shortly after the device is switched off and eradicated when the system restarts, and (ii) inaccessibility of the table which links serial numbers to the BUID.[110]

Neither TomTom nor anyone else can then, in principle, directly or indirectly identify the data subjects without disproportionate effort.[111] The *real-time* geolocation data is therefore no longer personal data within the meaning of Article 1, introduction and under a. of the Wbp.

4.3 Grounds

Pursuant to Article 8 of the Wbp the controller must have grounds for the data processing.

Article 8, introduction and under a. of the Wbp, states: *Personal data may only be processed if: (...)*
a. the data subject has unambiguously given his consent for the processing;

Pursuant to Article 1, introduction and under i. of the Wbp, consent must be "free", "specific" and "informed".

TomTom initially declared that all processes are based on the grounds of consent from the data subject.

In response to the report of provisional findings TomTom states that the processing does not concern personal data: *"Nevertheless TomTom has, for reasons of openness towards its customers, included a consent request, with regard to the collection of usage data by the device and the transfer to TomTom itself. On the basis of the experience gained,*

[108] See footnote 95.
[109] As of 27 April 2011 the link between serial numbers and the BUID is automatically deleted at the latest within 20 minutes after the device has been switched off. See footnote 59.
[110] TomTom letter dated 30 September 2011, Annex 3, p. 9.
[111] This applies except where the segmented data on routes driven is directly or indirectly traceable back to an individual user (for example because a route has been travelled at a less busy, different time in a thinly populated area).

TomTom has decided to add to the information provided."[112] And: *"Nevertheless, TomTom has decided, on the basis of the experience gained, to add to the information provided, and to include an explicit consent request prior to activating information uploads, for the purposes of the LIVE services."* [113]

Geolocation data on natural persons provide an intimate overview of someone's behaviour. This data is of a sensitive nature and may therefore only be processed with the unambiguous consent of the data subject. This was also recently confirmed in the opinion on geolocation data from the joint European supervisory bodies on the protection of personal data.[114]

As regards *historical* geolocation data, TomTom asks for prior consent for the collection of anonymous data to improve its products.

TomTom processes personal data, and not just anonymous data. The consent request is insufficiently specific on this point.

In addition, TomTom does not provide (sufficiently) clear information on the saving and storage of historical geolocation data on the device. TomTom cannot base this processing on unambiguous consent from the data subject.[115]

TomTom does not request separate consent for the collection and processing of *real-time* geolocation data prior to the use of the HD Traffic service, on *online* devices and in the smartphone application. The LIVE services are activated as standard when an *online* device is activated.[116] The data subject only sees a general reference to the TomTom privacy statement if he creates an account, that is at the moment that he links the device to the TomTom servers via his (own) computer connection.

The CBP has decided on several occasions that consent for the processing of personal data cannot be obtained via general terms and conditions.[117] This was confirmed in the opinion on consent issued by the joint European supervisory bodies on the protection of personal data.[118]

In the case of the smartphone application, however, some information is provided prior to its purchase, but the data subject is not explicitly informed about, for example, which data is sent with which frequency to TomTom.

[112] TomTom letter dated 30 September 2011, Annex 2, p. 7.

[113] Ditto, Annex 4, p. 11.

[114] WP29 185, Opinion 13/2011 on Geolocation services on smart mobile devices, 16 May 2011, URL: http://www.cbpweb.nl/downloads_int/wp185_en.pdf.

[115] See also p. 7 of WP29 187, Opinion 15/2011 on the definition of consent, 13 July 2011, URL: http://www.cbpweb.nl/downloads_int/wp187_en.pdf.

[116] Except in the case of devices which are permanently built into cars. TomTom letter dated 30 September 2011, Annex 5, p. 12.

[117] See for example CBP 8 April 2003, z2003-0316, URL: ww.cbpweb.nl/downloads_uit/z2003-0163.pdf and CBP, Findings on the investigation into Advance, December 2009, and in particular p. 27 and 28, URL: http://cbpweb.nl/downloads_pb/pb_20091218_advance_bevindingen.pdf.

[118] WP29 187, Opinion 15/2011 on the definition of consent, 13 July 2011, URL: http://www.cbpweb.nl/downloads_int/wp187_en.pdf.

In response to the report of provisional findings, TomTom stated: "*Although* [this does not constitute processing of data according to TomTom - added by the CBP], *TomTom has decided, on the basis of the experience gained, to add to the information provided, and to include an explicit consent request prior to activating information uploads, for the purposes of the LIVE services." It will also be possible to withdraw the consent at any time and reissue it. Withdrawing the consent will also have the consequence that the LIVE services will not be supplied. After all, it is impossible to supply this type of location based services without receiving location data."*

TomTom has stated that the consent request prior to the processing has since been included in the new *online* devices that are to be built in.[119]

According to the screen shots/texts and accompanying information which TomTom provided to the CBP on 28 November and 8 December 2011, the *online* devices contain a (new) consent request after installation of a software update. The question is accompanied by an additional clarification about the data which TomTom collects and processes and the data that is saved and stored on the device itself (historical and *real-time* geolocation data). The consent request on the *offline* devices will also be stated more precisely, with a clarification which specifies that historical geolocation data is recorded and stored on the device and which data TomTom collects. The same clarification will be made for the current iPhone application [CONFIDENTIAL] (or: a more detailed clarification of the data which TomTom collects and processes).

The software update for the *offline* and *online* devices and the smartphone application will be made available to users in the second half of February 2012.[120]

TomTom expects that the majority of users in the Netherlands will install this software within two to three months, for both the *offline* and *online* devices and the smartphone application.[121]

Because of the lack of unambiguous consent for the processing of *historical* and *real-time* geolocation data on current *offline* and *online* devices and the smartphone application, TomTom acts contrary to Article 8 of the Wbp (grounds).

In response to the report of provisional findings, TomTom has announced that the consent request and accompanying information will be expanded and made more precise on both sorts of devices and the smartphone application. An initial assessment shows that if TomTom implements these changes in the way of providing information and requesting consent, the observed violations will cease. A definitive assessment will follow as soon as possible after TomTom has actually implemented this.

[119] TomTom letter dated 30 September 2011, Annex 4, p. 11.

[120] TomTom letter dated 8 December 2011, p. 1.

[121] See footnote 40.

4.4 Further processing

Article 9 of the Wbp states: "*Personal data is not further processed in a way that is incompatible with the purposes for which it was acquired*" and the second paragraph contains a number of criteria for that assessment.

TomTom provides historical journey data only in aggregated form to third parties, such as local and provincial authorities, Eindhoven Airport and the Via.nl traffic advice bureau. Before the data ends up in the archive, the unique numbers or other identifying features of (the user of) the device or the smartphone application are removed in a number of phases and data processing systems. TomTom does not provide the data from the archive in rough form, but at an aggregated level, and also processes this for its own purposes to improve map material only in that form. At this aggregated level the data cannot (any longer) be reasonably directly or indirectly traced to natural persons, either by TomTom or another party. This is therefore, in this context, not personal data within the meaning of Article 1, introduction and under a. of the Wbp. The Wbp therefore does not apply to the provision of this data.

5. Conclusion

TomTom collects historical geolocation data from users via the *offline* version of the devices. TomTom collects *real-time* geolocation data from users via the *online* version and the smartphone application. TomTom also collects historical geolocation data via the *online* devices.

As regards historical geolocation data, TomTom asks users of *offline* and *online* devices for consent in advance to collect *anonymous data* to improve its products. TomTom processes personal data, and not just anonymous data. For this reason the consent request is insufficiently specific on this point. In its information to users TomTom does not make it (sufficiently) clear that the device saves and stores detailed historical geolocation data and that TomTom collects this file when the user connects with the TomTom servers.

The fact that TomTom has taken technical and organisational measures to prevent the identification of individual persons as much as possible does not lead to the conclusion that the data is not personal data. In view of its technical (decryption) possibilities and the current computation power of computers, TomTom must be considered to be capable of decrypting the file with geolocation data – without disproportionate effort – and of linking it to other identifying data of the data subject (such as name, e-mail address, etc.).

As regards *real-time* geolocation data, TomTom never asks users of *online* devices for consent to collect and process the combination of geolocation data with additional data such as the serial number and account name. In the case of the online version the data subject only sees a general reference to the TomTom privacy statement if he creates an account, that is at the moment that he connects the device to the TomTom servers via his (own) computer connection.

However no consent can be obtained for the processing of personal data via a privacy statement. In the case of the smartphone application, TomTom does provide some information prior to the purchase thereof, but the data subject is not explicitly informed about, for example, which data is sent with which frequency to TomTom.

TomTom acts contrary to Article 8 of the Wbp because of the lack of grounds.

In response to the report of provisional findings, TomTom has announced that the consent request and accompanying information will be expanded and made more precise on both sorts of devices and the smartphone application. An initial assessment shows that if TomTom implements these changes in the way of providing information and requesting consent, the observed violations will cease. A definitive assessment will follow as soon as possible after TomTom has actually implemented this.

TomTom provides data from the historical journey archive to third parties. Given that TomTom irreversibly removes identifying features from the data in the archive, and then only provides it at an aggregated level to third parties, the data is not personal data. The Wbp therefore does not apply to the provision of this data.