Margus Tiru
OÜ Positium LBS
Margus.tiru@positium.ee

7 January 2014

MEMORANDUM ON LEGAL REGULATION ON THE USE OF MOBILE POSITIONING DATA IN THE EUROPEAN UNION AND ESTONIA, FINLAND, GERMANY AND FRANCE

Feasibility study on the use of mobile positioning data for tourism statistics Eurostat contract No. 30501.2012.001-2012.452

Dear Margus,

This memorandum sets out the legal framework concerning the feasibility study on the use of mobile positioning data for tourism statistics (Eurostat contract No. 30501.2012.001-2012.452) (hereinafter the **Study**). The memorandum covers the legal implication on the level of the European Union (hereinafter the **EU**) and Estonia, Finland, Germany and France. Attorneys at law Borenius has collected and incorporated herein the memorandums of all participating countries but due to not being competent on foreign jurisdiction law does not assume liability for the correctness of the input provided by local counsel in Finland, Germany and France all of who have been contracted by OÜ Positium LBS directly and are therefore liable to Positium according to the terms of their respective contracts.

As instructed, the memorandum is structured by first giving a list of the relevant EU legal acts and the subject matter governed by them. This is followed by sections mapping the relevant laws of each involved sample jurisdiction providing the general framework as well as a short overview of the applicable rules. Thirdly, we have provided a chapter discussing in more detail the main issues of concern that arose during conducting the analysis. The memorandum is summed up by drawing conclusions based on the jurisdictions and implementation practice in sample countries as well as giving recommendations on what additional measures should be taken in order to clarify the applicable legal framework and eliminate risks highlighted.

1 INTRODUCTION

The legal framework governing the use of location data within the European Union is rather complex despite having the two directives of the European Parliament and of the Council directly governing the topic under discussion in force for a while already. The complexity of ever developing technological solutions used and business models applied leads to difficulties in categorisation of actual services and players in commercial chains according to the directives and relevant local laws. At the same time the lawfulness of data processing largely depends on such categorisation. An overview on the relevant EU legislation, the legislation of the four sample EU member countries as well as analysis of the major issues of concern is given below.

Where reference is made to the consultations with the Estonian Data Protection

Authorities such reference is to be understood as having been made to a meeting held with the four appointed officials of the relevant authorities expressing their views in verbal consultations. Therefore, although we have every reason to believe that the respective officials acted in their best competence and in good faith, any such opinions cannot be relied upon as the official opinions given by the Estonia Data Protection Authorities. Thus, we have given recommendations in this memorandum to further consult the data protection authorities of both Estonia and each other relevant Member State for obtaining further clarity on their views of interpreting the applicable laws.

2 EUROPEAN UNION LEGISLATION

Effective Instruments

The currently effective legal acts on the EU level directly relevant to the topic at hand are the following:

2.1 *Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the DPD);*

Also referred to as the "Data Protection Directive", the DPD is the fundamental instrument for the protection of personal data in the EU setting out the concept of personal data as well as the general principles and rules on the processing of such data. The DPD applies in every case where personal data are being processed as a result of the processing of location data.

2.2 *Directive 2002/58/EC (as amended by 2009/136/EC) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter the **EPD**).*

Also referred to as the "E-privacy Directive" the directive deals with privacy and personal data protection matters in the electronic communications sector. Consequently, the EPD only applies to the processing of the data processed by the telecom operators supplementing and specifying the DPD in aspects specific to the telecommunications sector.

2.3 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter the **DRD**).*

Also referred to as the "Data Retention Directive", the directive requires electronic communications operators to store certain categories of their customers' data for a period of six months to two years to make them available, upon request, to law enforcement authorities for the purposes of the investigation, detection and prosecution of serious crime.

2.4 *Article 29 Data Protection Working Party Opinion 13/2011 of 16 May 2011 on Geolocation services on smart mobile devices (hereinafter the **WP29 Geolocation Opinion**)*

The Article 29 Data Protection Working Party (hereinafter the **Working Party**) is a body set up under Article 29 of the DPD consisting of a representative of the supervisory authorities of each Member State, the European Data Protection Supervisor, and of a representative of the European Commission. The Working Party has advisory status and acts independently. Among other, the Working Party examines any question covering the application of the national measures adopted under the DPD in order to contribute to the uniform application of such measures as well as makes recommendations, on its own initiative, on all matters relating to the protection of persons with regard to the processing of personal data in the Community. The opinions of the Working Party are of advisory nature. However, since the Working Party is composed of the representatives of the supervisory authorities on both the EU and member states level, the Working Party's opinions should be regarded as reflecting the current position on data protection issues of the supervisory authorities on applying the effective legal acts. Therefore, it is recommended to take note of the Working Party's opinions including the WP29 Geolocation Opinion. As to the use of the geolocation data, the WP29 Geolocation Opinion is the main document addressing respective issue in detail in light of the relevant EU directives in force.

In addition to the above listed instruments there are others that govern certain issues that may be of relevance in terms of the use of mobile positioning data. References to such legal acts or other documents are made in the report where appropriate.

Proposed Instruments

2.5 *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (hereinafter the **Draft Regulation**).*

In addition to the legislation in force it should be taken into account that the European Commission has initiated the EU data protection reform by way of disclosing the said proposal for a new regulation that is also referred to as the General Data Protection Regulation.

Although the Draft Regulation contains, as does the DPD, a special article on the processing of personal data for statistics purposes, it must be noted that the Draft Regulation in its current working version does not add too much clarity as to the terms governing the processing of location data.

Although the language of the Draft Regulation makes use of the term 'location data', as opposed to the DPD, it is used only to indicate that location data may but need not necessarily be considered personal data. Accordingly, Recital 24) stipulates the following: "When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such should not be considered as personal data if they do not identify an individual or make an individual identifiable". Thus, it can be concluded that in the view of the European Commission the location data may but

need not be personal data. The categorization depends on specific circumstances of each case the data is processed.

Moreover, Art 4 (1) of the Draft Regulation uses location data as one type of data via which a data subject can be identified setting out the following: „'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, **location data**, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The processing of personal data for official statistics purposes is mainly governed by Art 83 of the Draft Regulation. Pursuant to Art 83 the personal data may be processed for historical, statistical or scientific research purposes only if:

(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

It is to be considered that the bodies conducting statistical research may publish or otherwise publicly disclose personal data only if:

(a) the data subject has given consent;

(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or

(c) the data subject has made the data public.

The Draft Regulation further stipulates that the European Commission shall be empowered to adopt delegated acts for the purpose of further specifying the criteria and requirements for the processing of personal data for the statistics purposes as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Therefore, although it can be presumed that by Art 83 the legislator indicates that it considers it essential to enable the processing of personal data for statistics purposes on special, and somewhat less strict conditions than those applying to the processing of the same for private purposes, the specific criteria and requirements are still to be set forth by the European Commission by adopting the delegated acts.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) voted on the Draft Regulation on 21 October 2013. The European Commission currently aims to update the current EU data protection legislation before the next European elections in May 2014 and the regulation is planned to take effect in 2016 after a transition period of two years. However, this entails reaching a trilateral agreement on the final version by the European Parliament, the Council and the Commission as well as the final vote by the European Parliament which is why it is currently unclear when exactly the Draft Regulation is going to be adopted.

General Overview of Legal Framework

2.6 *Main concepts of personal data protection*

2.6.1 *Personal data*

Pursuant to the DPD personal data is any information relating to an identified or identifiable natural person (a data subject) whereas an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Consequently, the DPD applies to processing of any information that relates to an individual that is identifiable by way of such information or data that is being processed.

In terms of the use of the mobile positioning data it is therefore first essential to identify if the data used qualifies as personal data or not. The DPD (among other, the obligation to obtain a data subject's consent for any type of data processing) does not apply in case the mobile positioning data collected and otherwise processed does not qualify as personal data.

The Study addresses the processing of anonymous and aggregated data. In order to preclude the applicability of the DPD one must determine that the mobile positioning data collected and otherwise processed is at all times throughout the process anonymous and that it cannot at any point be tracked down to an identifiable data subject. Please refer to Section 7.2 below for further analysis.

In each case where the data collected qualifies as personal data, the provisions of the DPD must be adhered to. These include, among other, the obligation to make sure that data is processed on one of the lawful basis set out in Section 2.6.4 below.

2.6.2 *Processing of personal data*

Under the DPD processing of personal data is to be understood as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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.

Resulting from the above, if the mobile positioning data qualify as personal data at any given point of time, any operations relating to such data (incl. collection, storing, using, etc.) constitutes the processing of personal data and can only be done in strict compliance with the DPD.

2.6.3 *Data controller and data processor*

Under the DPD a data controller is to be understood as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller is considered a data processor.

Making the distinction between a data controller and a data processor is essential since the data controller must procure that the processing of personal data is conducted according to the law. The data controller must also procure that the data processor that processes personal data on behalf of the controller does so in compliance with the law.

In light of the Study at hand, it should be identified which parties involved in the process of positioning data collection and use are considered data controllers and which of them data processors. Based on such identification of function the rights and obligations of each stakeholder can be determined.

2.6.4 *Lawful bases of processing personal data*

The general principle applying to personal data processing in the EU is that the processing is allowed on a data subject's due consent or in case a statutory basis for using the personal data without a data subject's consent exists. Such two conceptual bases have been set out in more detail in Art 7 of the DPD under which personal data may be processed only if:

(a) the data subject has unambiguously given his or her consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) of the DPD.

Therefore, unless specific statutory bases for processing exist, a data subject's consent should be obtained for each type of data processing in case the mobile positioning data qualify as personal data.

The specific statutory bases relevant in the context of processing personal data by the state statistics authorities is that set out in Section 2.6.4 (e) above – processing of personal data is necessary for the performance of a task carried out in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed.

Therefore, as a rule, the state statistics authorities as the data controllers may process personal data for the performance of a task in the exercise of official authority vested in them. However, the local laws are not that unambiguous concerning the applicability of such ground (refer to Section 7.3 for details).

2.6.5 *"Ownership" of data*

From the legal perspective the ownership of personal data is to be understood as a person's right to store, use or otherwise process the personal data relating to a data subject. Such right originally lies with the data subject who may determine the terms and conditions of his or her personal data by others. Such determination is made by way of a data subject's consent for processing his or her personal data. Additionally, personal data may be used according to the consent given by the data subject or under the law if the latter provides such specific basis.

When determining the rights to data other than personal data it must be taken into account that the mobile positioning data generally constitutes facts and other factual data. Facts and information as such are not protected by copyright. It is likely, however, that the owner of the database containing such facts or information enjoys the protection of a database owner. Since the use of the database owner's rights is a matter to be contractually handled between the owner of a database (e.g. a MNO) and the user of a database (e.g. data broker, Eurostat, etc.) and it does not involve consideration of statutory rights of a data subject, we do not focus on the database licensing rights in this memorandum to further extent.

2.6.6 *Location data and traffic data and processing thereof*

According to Art 2 (c) of the EPD **location data** means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Recital (14) of the EDP stipulates that **location data** may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

Pursuant to Art 2 (b) of the EPD **traffic data** is defined as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

Under Art 9 (1) of the EDP location data other than traffic data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service (refer to Section 2.6.7 below for the value added services). The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication (EPD, Art 9 (2)).

Processing of location data other than traffic data in accordance with Art 9 (1) and (2) must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third

party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication except as follows:

(a) traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued;

(b) certain traffic data may be used for the purpose of marketing electronic communications services or for the provision of value added services if the subscriber or user to whom the data relate has given his/her consent.

2.6.7 *Value added services*

Pursuant to Art 2 (g) of the EPD a value added service means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.

2.6.8 *Mobile operators' obligation to retain certain customer data*

Pursuant to Art 1 (2) of the DRD the latter applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user.

Under Art 4 of the DRD the Member States must adopt measures to ensure that data retained in accordance with the DRD are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) as interpreted by the European Court of Human Rights. Therefore, the extent and terms on which the data retained by the MNOs may be disclosed to third persons, including the competent authorities, must be stipulated by each local Member State law.

According to Art 5 of the DRD the following categories of data are to be retained concerning mobile telephony:

(a) data necessary to trace and identify the source of a communication

  (i) the calling telephone number;
  (ii) the name and address of the subscriber or registered user;

(b) data necessary to identify the destination of a communication:

  (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
  (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(c) data necessary to identify the date, time and duration of a communication:

(i) the date and time of the start and end of the communication;

(d) data necessary to identify the type of communication:

(i) the telephone service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(i) the calling and called telephone numbers;
(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;
(iii) the International Mobile Equipment Identity (IMEI) of the calling party;
(iv) the IMSI of the called party;
(v) the IMEI of the called party;
(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(f) data necessary to identify the location of mobile communication equipment:

(i) the location label (Cell ID) at the start of the communication;
(ii) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

The listed data must be retained by the communications services providers for the period of six months to two years as from the date of communication. The exact terms of data retention within this range are to be enacted by Member States in their local laws.

It is important to note that the data retained according to the DRD are subject to all requirements of personal data processing and the retention thereof does not release the data controller from adhering thereto, i.e. the retained data cannot be processed (in any other way that the retaining thereof) without the data subject's due consent or under express statutory basis.

3 ESTONIAN LEGISLATION

The following Estonian legal acts are applicable to the collection and use of mobile positioning data:

3.1 *Personal Data Protection Act (hereinafter the **PDPA**)*

The PDPA is the instrument by which the DPD has been transposed into Estonian law. The PDPA sets out the main terms and principles of processing personal data in line with the DPD.

3.2 *Electronic Communications Act (hereinafter the **ECA**)*

The ECA is the instrument by which the EPD and the DRD have been transposed into Estonian law. The ECA sets out general rules of processing subscribers' location data by mobile operators.

General Overview of Legal Framework

Pursuant to Art 105 (1) of the ECA a communications undertaking has the right to process subscribers' location data, the processing of which is not provided for in Art 104 (data necessary for billing the subscriber) or Art 111^1 (data subject to data retention obligation) of the ECA, only if such data are rendered anonymous prior to processing.

A communications undertaking (an MNO) may also process, with the consent of the subscriber, the data provided for in the previous paragraph to provide other services in the process of using the communications services to an extent and during the term necessary for processing and without rendering the data anonymous.

Data retention obligation

Under Art 111^1 (1) of the ECA any communications undertaking is required to retain the data that are necessary for the performance of the following acts:

1) tracing and identification of the source of communication;
2) identification of the destination of communication;
3) identification of the date, time and duration of communication;
4) identification of the type of communications service;
5) identification of the terminal equipment or presumable terminal equipment of a user of communications services;
6) determining of the location of the terminal equipment.

More specifically, the providers of mobile telephone services and mobile telephone network services are required to preserve the following data:

1) the number of the caller and the subscriber's name and address;
2) the number of the recipient and the subscriber's name and address;
3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address;
4) the date and time of the beginning and end of the call;
5) the telephone or mobile telephone service used;
6) the international mobile subscriber identity (IMSI) of the caller and the recipient;
7) the international mobile equipment identity (IMEI) of the caller and the recipient;
8) the cell ID at the time of setting up the call;
9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;
10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

The data must be retained for one year from the date of the communication if such data are generated or processed in the process of provision of communications services.

The data controller must ensure that the processing of the retained data complies with general personal data processing rules. Therefore an MNO may process the data that the MNO must retain under the data retention obligation in compliance with general personal data processing rules. Hence, the retained data may be processed if the data subject has given a consent or if there is a specific statutory basis for such processing.

3.3 *Official Statistics Act (hereinafter the **OSA**)*

The OSA governs the use of personal data in production of official statistics. Under Section 31 of the OSA a producer of official statistics has the right to use personal data on the bases of and pursuant to the procedure provided for in the PDPA in the production of official statistics. A producer of official statistics is not required to inform data subjects of the use of their personal data in producing official statistics. Please refer to Section 7.3 on the provisions of the PDPA relating to the processing of the personal data for the purposes of official statistics and relation thereof to Section 31 of the OSA.

4 GERMAN LEGISLATION

The following German legal acts are applicable to the collection and use of mobile positioning data:

4.1 *Federal Data Protection Act (hereinafter the **BDSG**)*

The BDSG sets out the main terms and conditions as well as the general principles of processing personal data in Germany. The BDSG constitutes the instrument of transposition of the DPD into German law.

General Overview of the Legal Framework

According to Art 4 (1) of the BDSG the collection, processing and the use of personal data shall be lawful only if permitted or ordered by the BDSG or any other law, or if the data subject has provided its consent.

Personal data means any information concerning the personal or material circumstances of an identified or identifiable natural person (a data subject). If information is anonymized (with no possibility to re-identify the respective person), the limitations and requirements of data protection, in particular those arising under the BDSG, are not applicable.

Under Art 3 (6) of the BDSG "rendering anonymous" is the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person or that such attribution would require a disproportionate amount of time, expense and effort. There is no specific case law available providing guidelines as to what is deemed a disproportionate effort. However, the common understanding is that a conservative and strict approach is to be taken upon construing the said concept with even the slightest possibility to re-identify the natural person prevents the qualification of data as anonymous data.

Where other federal laws apply to the processing of personal data, such as the TKG, they take precedence over the provisions of the BDSG.

4.2 *Telecommunications Act (hereinafter the **TKG**)*

The TKG sets out the main terms and conditions, as well as the general principles of the rights and obligations regarding the provision of telecommunication services in Germany. It also contains special provisions for processing personal data which are related to telecommunication. The TKG transposes the EPD into German law for telecommunication related issues.

The TKG also used to be the instrument by which the DRD was transposed into German law. However, due to a decision of the Federal Constitutional Court of Germany of March 2, 2010, the clauses which determined the conditions for the obligation of electronic communication operators to store certain categories of personal data to make them available, upon request, to law enforcement authorities for the purposes of the investigation, detection and prosecution of serious crimes, have been considered as a violation of the German Constitution and in consequence revoked and declared invalid.

Despite several legislative initiatives and a pending action of the European Commission before the European Court of Justice, Germany has still not transposed the DRD into German law.

General Overview of the Legal Framework

Art 96 (1) No. 1 of the TKG stipulates that the service provider itself may, without the data subject's consent, collect and use the following traffic data to the extent required for the purposes of establishing, framing the contents of, modifying or terminating a contract for telecommunications services:

1) number or other identification of the telecommunication connections involved or of the terminal equipment, personal authorisation codes, card number (if customer cards are used) and additionally, when mobile devices are used, the location data;
2) start and end of the connection, indicated by date and time and, if relevant for charging purposes, the volume of data transmitted;
3) telecommunication service used by the user;
4) termination points of fixed connections, beginning and end of their use, indicated by date and time and, if relevant for charging purposes, the volume of data transmitted;
5) any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes.

Without the traffic data stored by the telecommunications service provider the personal data may be used after the termination of a connection only when required to set up a further connection or for the purposes of:

1) invoicing of the services (Art 97 TKG);
2) provision of an itemized bill (Art 99 TKG);
3) identification and elimination of faults and malfunctions, identification of misuse (Art 100 TKG);
4) call tracing in case of telephone stalking (Art 101 TKG).

Otherwise traffic data are to be erased by the service provider without undue delay after the termination of the connection.

Special limitations regarding the use of location data which is not traffic data are contained in Art 98 of the TKG. According thereto location data relating to users of public telecommunications networks or publicly available telecommunications services may only be processed when made anonymous or with the customer's consent to the extent and for the duration necessary for the provision of value added services. In this case the service provider has to send a text message to the respective mobile device each time the respective device is being located if the location data is being displayed on a device other than the located mobile device. If location data is transmitted to a third party (other than the provider of the value-added service) the customer's consent has to be

declared in writing, which in this case does not include electronic form (Art 98 (1) 4) of the TKG). The consent may be withdrawn at any time.

Art 98 of the TKG does not allow the collection and processing of location data for statistical purposes. This stipulation solely allows the transfer of this type of data for the purpose of offering a value added service to the extent that such data is necessary to provide the respective service.

As long as location data has to be considered personal data, there is no legislative authorization in the TKG for collecting and processing such data for statistical purposes.

4.3 *Telemedia Act (hereinafter the **TMG**)*

The TMG incorporates the rules which constitute the transposition of the EPD into German law concerning personal data which is processed in connection with electronic information and communication services which are not telecommunication services exclusively consisting of the transmission of signals via telecommunication networks and which are not telecommunication-based services. In the relevant case of tourism statistics the TMG does not apply as long as the location data is being processed by a telecommunication service provider. The TMG, however, would be applicable if the location data originates from another source, such as provision of internet services, even if the internet is been accessed via a mobile device.

4.4 *Federal Statistics Act (hereinafter the **BStatG**)*

The BStatG regulates the terms and conditions of the collection, processing, presenting and analysing of data concerning mass phenomena in order to provide statistics for federal purposes.

General Overview of the Legal Framework

According to Art 5 (1) of the BStatG federal statistics shall principally be ordered by law or in certain cases by federal ordinance ("Rechtsverordnung"). Art 18 of the BStatG stipulates that the BStatG shall also be applicable in case of a statistical survey by the European Union, provided that the respective European law does not state otherwise. Art 19 of the BStatG enables the Federal Statistical Office to participate in statistical programs or the elaboration of statistics of the European Union or international organizations.

Regarding the processing of personal data in connection with a statistical evaluation Art 16 of the BStatG contains detailed confidentiality obligations. Such data has to be kept strictly confidential unless:

(a) the respective person has agreed to the contrary in writing;

(b) the data has been obtained from a source available to the public or from an official source named in Art 15 (1) of the BStatG if the obligation to provide information derives from a law ordering federal statistics;

(c) the data is combined by the federal statistics agency or a state statistics agency with data referring to other individuals and presented in a statistical conclusion;

(d) the data cannot be associated with the respective person.

Therefore the confidentiality obligation does not apply if the information cannot be attributed to an individual person, hence, if the data is anonymized. According to Art 21 of the BStatG the combination of data from statistics with other information in order to re-identify individual persons for other reasons than statistical purposes or any other purpose accepted by the federal law ordering the statistic is forbidden.

The transfer of personal data between persons or entities appointed with the preparation of federal statistics is allowed as far as necessary for such purpose. The owner of the data can be obliged to cooperate and provide the requested data by law (Art 15 of the BStatG). According to Art 17 of the BStatG the relevant persons have to be informed about the purpose of the statistics and about their statutory rights in this regard.

5 FRENCH LEGISLATION

The following French legal acts are applicable to the collection and use of location data:

5.1 *Information Technology, Data Files and Civil Liberties Act (hereinafter the **ITLA**)*

The ITLA transposed the DPD into French law and sets out the main terms and conditions concerning the protection of personal data in France. The French data protection regulator (hereinafter the **CNIL**) also regularly issues recommendations and guidelines. Such recommendations and guidelines are not mandatory rules but should generally be followed unless this is justified by a legitimate ground and in compliance with the ITLA.

Personal data

According to Section 2 (2) of the ITLA, personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

Location data is generally considered by the CNIL as personal data, insofar as it can be related to the subscriber of an electronic communications service.

Anonymous data

Anonymous data is not defined as such by the ITLA but the CNIL issued guidelines on anonymization in its 2010 Guide on Security of Personal Data (Factsheet No. 16).

In order not to be subject to the ITLA, processing of personal data must be subject to an irreversible anonymization, which consists in removing any identifying character from a set of data. This means that all directly and indirectly identifying information is removed and that it is impossible to re-identify the persons. The CNIL recommends to:

- be very careful insofar as re-identification can take place from partial information;
- proceed as follows to anonymize personal data:
    - generate a secret that is long enough and difficult to memorize;
    - apply a "one-way" function to the data: an algorithm suitable for such an operation is a keyed hash function such as the HMAC algorithm based on SHA-1.

The CNIL considers that anonymization mechanisms that have not been validated by experts should not be used. In particular a good anonymization algorithm must:

- be irreversible;
- present a very weak collision rate: two different data should not lead to the same result;
- present a great dispersion: two quasi-similar data must have very different results;
- use a secret key.

In some cases the CNIL considers that a double reversible anonymization is advisable, i.e. the application of a second anonymization on the result of a first anonymization, both anonymizations using different secrets, held by separate organisations. The FOIN algorithm (*Fonction d'Occultation des Informations Nominatives*, Personal Information Hiding Function) is an example of algorithm using double anonymization.

General Overview of Legal Framework

The principles according to which personal data can be lawfully processed are the same as the principles set out by the DPD.

In particular, Art 6 (2) of the ITLA provides that the data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. However, further data processing for statistical, scientific and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is carried out in conformity with the principles and procedures provided for in Chapter II of the ITLA (conditions for a lawful data processing which are similar to the conditions set out in the DPD), in Chapter IV (formalities, e.g. notifications, prior to commencing data processing) and in Art 1 of Chapter V (obligations incumbent upon data controllers and rights of data subjects, mainly relating to the information of the data subjects, the security of the data and the retention duration) and if it is not used to take decisions with respect to the data subjects.

The consent of the data subject is necessary for the processing of his data, under the same conditions as those set out in the DPD.

In this respect, under Art 6 of the ITLA, consent of the data subject is not necessary for data processing relating to compliance with any legal obligation to which the data controller is subject or the performance of a public service mission entrusted to the data controller or data recipient.

Notification

If the data is not anonymized when transferred to the statistics authorities and the processing is therefore subject to the ITLA, a standard notification should be filed with the CNIL by the data controller describing, notably, the purpose of the processing, the categories of data subject to the processing, together with the recipients and the retention duration, the security and confidentiality measures in place and how the data subjects are informed of their rights. The data processing cannot commence before receiving the CNIL's receipt of such notification. In the case contemplated herein, the statistic authorities could be considered as data controller.

The notification does not exempt the data controller from respecting its other obligations, in particular from obtaining the data subjects' consent when necessary.

Prior authorizations are necessary for some data processing (in particular in case of sensitive data processing, interconnection of databases having different purposes,

transfers outside of the European Union or processing used to take decisions regarding the data subjects). This point should be further reviewed, but if the intent is to only transfer identification data and location data for statistical purposes and the data remains within the European Union, no specific authorization should be necessary.

Information of the data subjects

Art 32.III of the ITLA provides that whenever the data have not been obtained from the data subject, the data controller or its representative must at the time of recording the personal data or, if disclosure to a third party is planned, no later than the time when the data are first disclosed, provide the data subject with the following information:

- the identity of the data controller and of his representative, if any;
- the purposes of the processing for which the data are intended;
- whether replies to the questions are compulsory or optional;
- the possible consequences for him of the absence of a reply;
- the recipients or categories of recipients of the data;
- the rights of individuals in relation to the processing of data (i.e. right of access, rectification and opposition);
- when applicable, the intended transfer of personal data to state that is not a Member State of the EU.

When the personal data have initially been obtained for another purpose, the above provisions shall not apply to processing necessary for the storage of these data for historical, statistical and scientific purposes, under the conditions provided for in Book II of the Heritage Code or for the re-use of these data for statistical purposes under the conditions provided for in Art 7 bis of Act No. 51-711 of 7 June 1951 on obligations, co-ordination and confidentiality as regards statistics. Book II of the Heritage Code relates to archiving of data and Art 7 bis of Act No. 51-711 relates to the assignment to the French state statistic authorities of personal data collected by a public or private entity managing a public service.

In addition, the above obligations of information do not apply whenever the data subject has already been informed or whenever informing the data subject proves impossible or would involve disproportionate efforts compared with the interest of the procedure.

Finally, Art 32.IV of the ITLA provides that if the personal data obtained are, within a short period of time, to form part of an anonymization procedure that was recognized beforehand by the CNIL as complying with the provisions of the ITLA, the information delivered by the data controller to the data subject may be limited to that mentioned in subsections 1 and 2 above.

Art 38.II of the ITLA also provides that the right of access of the data subjects is not applicable when the personal data is stored in a form that clearly excludes all risk of violating the privacy of the data subject and for a period that does not exceed that necessary for the sole purpose of creating statistics, or for scientific or historical research. Such exemptions by the data controller must be mentioned in the application for authorisation or in the notification addressed to the CNIL.

Retention duration

According to Art 36 of the ITLA, personal data may be stored beyond the period necessary for the purpose of the processing only for historical, statistical and scientific purposes. The choice of the data that is stored must be made, in such a case, in

accordance with the legal provisions relating to public data (Art L212-4 of the Heritage Code).

5.2 *Post and Electronic Communications Code (hereinafter the **PECC**)*

The PECC sets out the main terms and conditions applicable to electronic communications in France, including the processing of location data and other data collected by MNOs.

General overview of Legal Framework

The articles of the PECC relating to personal data processing apply to the providers of electronic communications services and to networks which are in charge of data and identification collection tools.

In accordance with Art L34-1.II of the PECC, the MNOs must erase or make anonymous any data relating to traffic, i.e. any information made available through electronic communications means that may be recorded by the MNO during the electronic communications transmitted though the MNO. The exceptions to such obligations are:

- data retention obligation, as described below,
- for invoicing purposes, for certain categories of data,
- for the purpose of providing value added services, as described below,
- for the location data, under certain conditions, as described below, and
- for some data, for the purpose of ensuring the security of their network.

Data retention obligation

MNOs are required to retain data (including location data), pursuant to Art L34-1.III of the PECC, but only for the purpose of searching, observing and prosecuting criminal offenses or a breach of copyrights, and such data can only be communicated to a judicial authority or the authority in charge of monitoring copyrights' breaches. Such data must be kept for only one year.

The data in question is not described herein, as it could not be used for the project contemplated in this memorandum.

Value added services and location data

Art L34-1.IV provides that MNOs can process the data relating to traffic for the purpose of commercializing their own electronic communications services or to provide added value service, only with the consent of the data subject and for a limited duration. Such duration cannot exceed the period necessary for the supply or commercialization of the services.

Art 34-1.V of the PECC also provides that location data cannot be used during communication for any purpose other than the routing of the same, nor be kept nor stored after the end of the communication without the consent of the user, duly informed of the categories of data in question, the duration of the processing, its purposes and the fact that such data will or not be transferred to third party service providers. The user must be able to withdraw his consent at any time without cost, except for the cost linked to the transmission of the withdrawal. The user must also be able to suspend his consent by a simple and free of charge mean, except for the cost linked to the transmission of such suspension. The prior consent of the data subject is consequently necessary for personal data to be transferred from the MNOs to the statistical authorities.

Art 34-1.VI of the PECC further provides that the data kept and processed under the above conditions (both under Art 34-1.IV and Art 34-1.V) can only exclusively concern the identification of the persons using the services provided by the MNOs, the technical characteristics of the users' communications and the location data.

They can in no case relate to the content of the exchanged correspondences or the information consulted by the users, in any form whatsoever, during such communications.

The processing of the data must also comply with the ITLA and the MNOs must take all appropriate measures to prevent use of the data for other purposes than the above.

6 FINNISH LEGISLATION

The following Finnish legal acts are applicable to the collection and use of mobile positioning data.

6.1 *Personal Data Act (hereinafter the **HTL**)*

The HTL is the instrument transposing the DPD into the Finnish legislation. It contains the terms and conditions and general principles of processing personal data in Finland.

General overview of the Legal Framework

The definitions used for personal data and the processing of personal data in the HTL are identical to the DPD. Art 8 (1) and (4) of the HTL set out general prerequisites to processing of personal data. The relevant prerequisites are:

(1) the data subject has unambiguously consented to the same;

(4) processing is based on the provisions of law or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of law or an order issued on the basis of law;

6.2 *Act on the Protection of Privacy in Electronic Communications (hereinafter the **SVTL**)*

The SVTL is the instrument by which the DRD is transposed into Finnish legislation. An amendment to the act was made in 2008 making it compliant with the DRD.

6.3 *The Statistics Act (hereinafter the **TL**)*

The TL lays down provisions on the procedures and principles concerning the collection of data and the designing and production of statistics that shall be applied by state authorities in their statistics compilation. The collection, release, protection and other processing of data during the compilation of statistics must be subject to the provisions of the Act on the Openness of Government Activities (621/1999) and of the Personal Data Act (523/1999), unless provided otherwise by the law.

On data collection Art 5 of the TL stipulates that the data must be collected and stored without identification data whenever permitted by the statistics to be produced. Identification data may only be collected and stored where it is necessary for data linking or when otherwise deemed necessary for the production of reliable and comparable statistics depicting features in the development of social conditions.

ARt 10 of the TL stipulates that when data collected for statistical purposes are being combined, stored, destroyed or otherwise processed it shall be ensured that no person's protection of private life or personal data, or business or professional secret shall be endangered.

Concerning the right of Statistics Finland to collect data from enterprises, Art 14 of the TL provides that they are obliged to provide Statistics Finland with data on the type, location, ownership, finances and products of their activities, as well as with data on the staff and other resources required in their activities. However, the obligation of enterprises does not extend to providing data on the users of their products or services. Therefore based on the current TL enterprises cannot be obliged to provide data on their client registers such as client positioning data collected by MNOs.

6.4 *Communications Market Act (hereinafter the **VML**)*

The objective of the VML is to promote the provision and use of services within communications networks and to ensure that communications networks and communications services are available under reasonable conditions to all telecommunications operators and users throughout the country.

The VML act established the legal framework for the operations of telecommunications service providers in Finland. It does not directly deal with issues regarding use of personal data or positioning data.

7 OVERVIEW OF MAIN ISSUES OF CONCERN

7.1 *Data necessary for the purposes of tourism statistics*

According to our understanding the following data is required or desirable for the purposes of conducting the tourism statistics:

- the calling telephone number;
- the name of the subscriber or registered user;
- the International Mobile Subscriber Identity (IMSI) of the calling party;
- the date and time of the start of the communication;
- the location label (Cell ID) at the start of the communication;
- data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained;
- the name and address of the subscriber or registered user;
- address of the subscriber;
- the date and time of the end of the communication (for the duration of the call);
- the telephone service used (type of the event, e.g. incoming call, outgoing SMS, location update, etc.);
- in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated.

All the above listed data constitute the data subject to the data retention obligation under the DRD (see Section 2.6.8 above). Hence, the required data must be retained by the MNOs as set out by each local law. Despite the obligation to retain the data (note the

exception of Germany described in Section 4.2 above) such data, if deemed personal data, may only be processed in any other way if the data subject has given his prior consent or if there is a specific statutory basis for such processing.

7.2 *Anonymous and aggregated mobile positioning data as personal data*

As explained in Section 2.6.1 above any data is considered personal data and is therefore within the scope of the DPD in case such data relates to an identified or identifiable natural person. The criteria of identifiability are further addressed in Section 3 of the Working Party Opinion 4/2007 On the Concept of Personal Data of 20 June 2007.

Moreover, the Working Party has stated in their Opinion on the Use of Location Data with a View to Providing Value-added Services as of November 2005 that since location data always relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in the DPD. Moreover, Section 4.1.1 of the Geolocation Opinion stipulates that since location data derived from base stations relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in the DPD.

Therefore, based on the Working Party opinions it should be concluded that the location data are always considered to be personal data, and therefore within the scope of the DPD.

Nevertheless, it must be taken into account that the Working Party opinions are of advisory rather than compulsory nature. Moreover, we are of the opinion that the position of automatically treating all location data as personal data is not fully correct.

Aggregated data

Based on information provided to us as the basis for carrying out this analysis we have presumed that the aggregated data cannot be traced down to an identifiable person at any time in any way. If such presumption is correct, it can be concluded that the processing (incl. collecting, storing, using, transmitting, etc.) of the aggregated mobile positioning data does not fall within the scope of the DPD and is therefore freely usable without any data protection implications by persons who obtain possession of such data in the aggregated form. This applies to the data brokers and other third persons that obtain the data in aggregated form from the MNOs.

It must be taken note of, however, that at the time of collecting the underlying data by an MNO the data is not yet in aggregated form. Therefore, collection and processing (rendering into aggregated form) of the data that can be traced down to an individual (a subscriber or user) by an MNO is deemed processing of personal data. Such processing by an MNO must therefore be conducted in accordance with the applicable laws.

It could be argued that if an MNO processes for the mere purpose of rendering into aggregated form of personal data that such MNO has in its disposal anyway such processing by the MNO should not be deemed to interfere with the relevant data subjects' privacy more than it would without said processing for such specific purpose. Certain representatives of the Estonian Data Protection Authorities have in course of verbal consultations opined the same. It must be taken into account, though, that formally there is no basis arising from the law that would support such interpretation. Therefore, in order for an MNO to act diligently, it should obtain due prior consents from relevant data subjects for the processing of their personal data for the described purpose. Given that obtaining the consents separately immediately prior to

commencement of relevant data processing is not practically feasible, it is recommended that respective consent is given by the client in the client agreement concluded with the MNO.

Anonymous data

The concept of anonymous data is somewhat more complex. It is our understanding that anonymous data may in principle be tracked down to an identifiable person although such possibilities are extremely limited. It needs to be clarified if such tracking down can be considered direct or indirect identifiability in light of the DPD and relevant local laws. The Working Party states in its Opinion 4/2007 on the Concept of Personal Data that "/…/ in general terms, a natural person can be considered as "identified" when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able"). This second alternative is therefore in practice the threshold condition determining whether information is within the scope of the third element".

In its Geolocation Opinion the Working Party has stated that "/…/ smart mobile devices are inextricably linked to natural persons. There is usually direct and indirect identifyability. First of all, the telecom operator providing GSM and mobile internet access usually has a register with the name, address and banking details of every customer, in combination with several unique numbers of the device, such as IMEI and IMSI. Secondly, the purchase of extra software for the device (applications or apps) usually requires a credit card number and thereby enriches the combination of the unique number(s) and the location data with directly identifying data. /.../ Indirect identifyability can be achieved through the combination of the unique number(s) of the device, in combination with one or more calculated locations. Every smart mobile device has at least one unique identifier, the MAC address".

It results from the above that any location data is personal data even if the relevant data subjects (MNO's customers) have not been but could in principle be identified based on such location data. Therefore, one should conclude that anonymous data (as opposed to aggregated data in the context of the Study), to the extent a person can be singled out based thereon, may only be processed by an MNO upon the customers' prior consent or on a basis set out by the law. Such conclusion is not affected by the fact that both the DPD and EPD use the term "anonymous" when referring to the state the data must be brought into for the purposes of the data controller being able to process thereof without the data subject's consent. In the context of the DPD and the EPD "anonymous data" is meant as data based on which a person cannot be singled out.

To conclude, the applicability of the DPD and the relevant local laws depends on whether the mobile positioning data constitutes personal data or not. In case the mobile positioning data does not relate to an identified or an identifiable individual and is of purely statistical nature, such data is not personal data and the DPD and the PDPA (and local laws implementing the DPD in their respective legislations) do not apply.

7.3 *Processing personal data for official statistics needs as a statutory basis for processing personal data*

If a data subject's consent is not obtained personal data may be processed only when a statutory basis for processing exists. Such statutory basis must be expressly set out by the law.

There are two possible bases whereon the personal data may potentially be processed for the purposes of official statistics.

First, the general statutory basis for the processing of personal data arises from Art 7 (e) of the DPD (processing data for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed). The prerequisite to applying this basis is that the state statistics authorities need the data in order to perform an official task given to them by law. Provided that the statistics authorities can request personal data from an MNO on such statutory basis, the MNO is obliged to transfer such requested data.

Second, the DPD also stipulates a more specific statutory basis in its Art 6 (b) under which Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

The implementation of Art 7 (e) and Art 6 (b) of the DPD in the investigated jurisdictions is varied.

Estonia

The OSA provides that a producer of official statistics may use personal data on the basis of and pursuant to the procedure provided for in the PDPA whereas he is not required to inform data subjects of the use of their personal data in producing official statistics. Therefore the OSA does not set out an individual basis for the state statistics authorities to process personal data for statistics purposes and the latter has to be done according to the PDPA as the general law.

Art 10 (2) of the PDPA transposes Art 7 (e) of the DPD into Estonian law. Thereby an administrative authority shall process personal data only in the course of performance of public duties in order to perform obligations prescribed by law. Furthermore, Art 14 (1) 1) and 2) of the PDPA stipulate that processing of personal data is permitted without the consent of a data subject if the personal data are to be processed on the basis of law or for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission.

The Estonian Data Protection Authorities have in course of verbal consultations expressed an opinion that Statistics Estonia should in principle be allowed to process personal data on this ground rather than on the grounds of Art 16 of the PDPA. It should be noted, though, that Art 10 (2) and Art 14 (1) 1) and 2) are of very general nature and do not specify the terms and conditions of such processing.

Art 16 of the PDPA transposes Art 6 (b) of the DPD into Estonian law. As opposed to Art 10 (2) and Art 14 (1) 1) and 2) Art 16 sets forth terms and conditions of such processing in further detail. Art 16 (1) stipulates that data concerning a data subject may be processed without the consent of the data subject for the needs of official statistics only in coded form. Before handing over data for processing it for the needs of official statistics, the data allowing a person to be identified shall be substituted by a code. Decoding and the possibility to decode is permitted only for the needs of additional official statistics. The controller of the personal data shall appoint a specific person who has access to the information allowing decoding.

The PDPA does not specify what a coded form of data means. The underlying EU directives do not use the term "coded form". It remains ambiguous where one should draw a line between the "coded" data and the data "in a format which does not enable identification of the data subject". We recommend holding further consultations with the Estonian Data Protection Authorities in this respect for clarification purposes.

Therefore, if an MNO as the data controller has collected its customers' location data it may transfer such to a government institution performing the function of producing official statistics even without the relevant data subjects' consent given that the data is in coded form. It does not follow clearly from the referred provision of the PDPA if the person that the MNO must appoint as the one having access to the decoding information must be an employee of the data controller or can also be a third person. Taking account of the general principles of personal data processing we are of the opinion that relevant provision should be construed conservatively to be understood as only an employee or other person acting under the control and supervision of a data controller can be granted access rights to the decoding data.

Art 16 of the PDPA further stipulates that processing of data concerning a data subject without the person's consent for official statistics purposes in a format which enables identification of the data subject is permitted only if, after removal of the data enabling identification, the goals of data processing would not be achievable or achievement thereof would be unreasonably difficult. In such case, the personal data of a data subject may be processed without the person's consent only if the person carrying out the scientific research finds that there is a predominant public interest for such processing and the volume of the obligations of the data subject is not changed on the basis of the processed personal data and the rights of the data subject are not excessively damaged in any other manner.

Although pro and contra arguments can evidently be found it would in our opinion be difficult to argue that processing of location data for the purposes of statistics producing reasons is a predominant public interest if the same result can be reached by alternative means (i.e. alternatively collected data).

It should be further borne in mind that the processing of personal data for official statistics purposes without the consent of the data subject is permitted if the data controller has taken sufficient organisational, physical and information technology security measures for the protection of the personal data, and if such processing involves processing of sensitive data, has registered the processing of sensitive personal data. The processing of such personal data can only be commenced if the Estonian Data Protection Authorities have verified compliance with the requirements set out in the law and, if an ethics committee has been founded based on law in the corresponding area, has also heard the opinion of such committee.

Collected personal data may be processed for the purposes of official statistics regardless of the purpose for which the personal data were initially collected. Personal data collected for official statistics may be stored in coded form for the purposes of using it later for scientific research or official statistics.

Based on the Estonian statutory regulation described above it must be concluded that it is not clear whether Art 16 of the PDPA serves as a specific rule in relation to the more general Art 10 (2) and Art 14 (1) 1) and 2). If it does, the processing of personal data by statistics authorities must be conducted pursuant to the provisions of Art 16. In case it does not, it remains unclear what terms and conditions the statistics authorities must adhere to upon processing data under Art 10 (2) [and Art 14 (1) 1) and 2)]as well as in

which case does Art 16 apply. In course of verbal consultations the Estonian Data Protection Authorities have indicated that in their opinion Art 10 (2) and Art (14 (1) 1) and 2) should be a sufficient basis for such processing. No further guidance was given though.

In case Art 10 (2) as well as Art 14 (1) 1) and 2) are to be considered an independent basis of processing data for statistics purposes, Statistics Estonia must be subject to a statutory obligation to collect and otherwise process the mobile positioning data to the extent relevant. Such obligation must arise from the law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission. The law does not clarify to what level of detail the obligation of Statistics Estonia should be set out by the law to be eligible under Art 10 (2) and Art 14 (1) 1) and 2) of the PDPA. Nor does the law specify based on which criteria it should be assessed whether specific data is necessary for the performance of a specific task (e.g. whether the data should be inevitably necessary for the performance of the task or is it sufficient if the performing of a task is easier, more efficient, etc. as a result of processing the data whereas the task could in principle be performed by taking alternative measures as well). The Estonian DPA has opined in course of verbal consultations that they do not expect the law should necessarily set forth an expressed obligation to collect mobile positioning data from MNOs or similar detailed obligation. Therefore, in principle, the general obligation of Statistics Estonia to produce official statistics arising from the OSA should be sufficient if Statistics Estonia provides sufficient arguments that it is not possible to produce required statistics without relevant location data.

Additionally to the obligation to perform official statistics arising from the OSA, Art 1 of the Regulation (EC) 692/2011 of the European Parliament and of the Council of 6 July 2011 concerning European statistics on tourism and repealing Council Directive 95/57/EC (hereinafter the **Regulation 692/2011**) stipulates that the Member States shall collect, compile, process and transmit harmonised statistics on tourism supply and demand, and elaborates on such obligation in its further provisions. Under Art 8 (b) of the same it can be concluded that the MNOs' databases of positioning data are acceptable sources of data for official statistics. The regulations of the European Parliament and the Council are directly applicable legal acts in the Member States. Therefore the provisions of the Regulation 692/2011 need not be transposed into Estonian law to be applicable locally. Therefore, the conclusion drawn herein supports the position that if Statistics Estonia needs the mobile positioning data in order to fulfil its task of producing official tourism statistics it may claim such data from the MNOs for processing thereof for such purpose. The latter conclusion is valid on the precondition that the data categories and intended use of the data is covered by the purposes determined in Art 3.1 of Regulation 692/2011. If those purposes do not require the use of positioning data the Commission could, according to Art 3.2 and 11 of Regulation 692/2011, adopt a delegated act in order to adapt this list of subjects and characteristics of the required data. With such act the commission could further extend the purposes included in Art. 3.1 of Regulation 692/2011 on statistical purposes, which require as source the MNOs' databases of positioning data.

It is more ambiguous, though, on which terms and conditions Statistics Estonia has to process the data, among other, whether the data should be aggregated or made anonymous at a certain point of time.

The Regulation (EC) 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation

(EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (hereinafter the **Regulation 223/2009**) sets out the rules of confidentiality of statistical data. 'Confidential data' in the context of the said Regulation means data which allow statistical units to be identified, either directly or indirectly, thereby disclosing individual information. To determine whether a statistical unit is identifiable, account shall be taken of all relevant means that might reasonably be used by a third party to identify the statistical unit. Therefore, the identification criteria of a statistical unit are, by large, similar to the criteria of identification of a data subject pursuant to the DPD. Under Art 3 6. a statistical unit may, among other, be a natural person or a household. Thus, it can be concluded that in principle the confidential data under Regulation 223/2009 may, in case of a natural person being the statistical unit, be data by which the natural person can be identified, i.e. personal data in the meaning of the DPD.

Pursuant to Art 20 2. of Regulation 223/2009 confidential data obtained exclusively for the production of European statistics shall be used by the national statistics authorities and other national authorities exclusively for statistical purposes unless the statistical unit has unambiguously given its consent to the use for any other purposes. Therefore, presuming that the confidential data in light of the Regulation can be deemed personal data, one possible conclusion would be that the authorities may process the personal data for statistical purposes without the data subject's consent. It needs to be taken into account though that Art 20 2. of Regulation 223/2009 applies to confidential data obtained exclusively for the production of European statistics. Therefore, it is questionable whether this applies to data that was originally collected by a third person (an MNO) for its business purposes and only thereafter transferred to be processed for statistical purposes.

The national statistics authorities must take all necessary measures to ensure the harmonisation of principles and guidelines as regards the physical and logical protection of confidential data. Those measures shall be adopted by the Commission in accordance with the regulatory procedure referred to in Article 27(2). Furthermore, officials and other staff of the relevant authorities having access to confidential data shall be subject to compliance with such confidentiality, even after cessation of their functions. Any transmission of confidential data by the national statistics authorities may only be conducted according to Article 21 of the Regulation 223/2009.

As far as the transfer by MNOs of personal data to Statistics Estonia is concerned, Art 14 (2) 1) of the PDPA stipulates that communication of personal data or granting access to personal data to third persons for the purposes of processing is permitted without the consent of the data subject if the third person to whom such data are communicated processes the personal data for the purposes of performing a task prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission. Thus, provided that Statistics Estonia needs such data in order to perform its official tasks under the OSA and the Regulation 692/2011 the MNOs are entitled and obliged to transfer such personal data to respective authorities.

In case the business model used involves transferring personal data by an MNO to a data broker or mediator rather than to Statistics Estonia directly, a question arises if such transfer of the data, even if eventually used for official statistics purposes, qualifies as lawful data transfer by an MNO. In order to eliminate the risk of the data brokers/mediators of illegal processing of personal data they should also be subject to performing a statutory task commissioned to them under the law or a contract under public law concluded with the state statistics authorities.

Due to the lack of relevant legal practice in Estonia it is recommended that the Estonian Data Protection Authorities are consulted in order to gain further clarity.

Germany

German law allows the processing of data for statistical purposes if a German or European law enables the Federal Statistical Office or a comparable European Authority to do so. The main requirement in this case is that the personal data is kept confidential, unless the data cannot be associated with the individual mobile phone user, i.e. by anonymizing the data and combining data referring to several users in a statistical conclusion. However, a law enabling the Federal Statistical Office to claim and process location data does not currently exist in Germany.

Provided that such law was enacted, the Federal Statistical Office could claim the transfer of such location data from any person incl. the MNOs. According to Art 17 of the BStatG the relevant persons have to be informed about the purpose of the statistics and about their statutory rights in this regard. The further conditions for the claim of location data would be determined in the respective legal provisions and, therefore, cannot be foreseen at this point of time.

According to the TKG location data which can be qualified as traffic data can only be stored by an MNO as long as such data is necessary for the purposes of invoicing for the services, provision of an itemized bill, the identification and elimination of faults and malfunctions, identification of misuse and call tracing in case of telephone stalking (Art 96 to 101 of the TKG). During this period the MNO could be obliged by respective law to transfer these personal location data for statistical reasons to the Federal Office for statistics.

If, however, an MNO stores location data for a longer period than needed for the above mentioned purposes, it has to anonymize the location data since the processing of such personal data is only allowed for the purposes described in Art 96 and 98 of the TKG.

The Regulations 692/2011 and 223/2009 are directly applicable in each member state of the European Union. Therefore, the conclusions drawn in this Section 7.3 above concerning the effect of these two regulations on the Estonian legal system are valid for the German jurisdiction as well.

Nevertheless, it is highly recommended that the German Data Protection Authorities are consulted regarding whether the anonymized location data still constitute personal data or not, if the establishing of a connection between these data and a certain person is theoretically possible but, due to the complexity and effort needed, effectively very improbable.

Finland

There are two three main issues of concern related to obtaining and using mobile positioning data for the purpose of producing tourism statistics in Finland.

First, the current Statistics Act obliges enterprises to provide data on their products and services but not on the clients consuming these products and services. Therefore the current Statistics Act does not oblige MNOs to provide mobile positioning data to Statistics Finland.

Secondly, according to the Act on the Protection of Privacy in Electronic Communications the identification data may only be processed by a natural person employed by or acting on behalf of a telecommunications operator.

The third key question is whether anonymous raw data provided by MNOs constitutes personal data or not under the HTL. The Data Protection Ombudsman, the main data protection authority in Finland, was consulted regarding this question and they stated that the raw data, although anonymized, still constitutes personal data. Thus there arises a need for a mediator to process the data into aggregated form on the premises of the MNO. Such mediator has to have access to the raw data maintained by the MNO as well as possess methodological competence and tools to process the raw data into aggregated data. This scenario involving a mediator is challenging technically, financially and in terms of organization.

France

The prerequisites for an MNO to be able to transfer location data deemed to be personal data to the statistics authorities would be the following.

Generally, for the transfer of personal data to the statistics authorities by an MNO, the MNO must itself lawfully process the data and respect all of its obligations as data controller. The data cannot be transferred by an MNO for statistics purposes without the prior consent of the data subject. Moreover, the MNO must have duly filed with the CNIL the notification corresponding to its data processing, mentioning the transfer of data to third parties, and must provide to users all mandatory information regarding such data processing.

The transfer agreement entered into between the statistics authorities and the MNO should provide that the MNO complies with the above. A copy of the MNO's notification(s) should also be requested.

Pursuant to Art 34-1.VI of the PECC, the MNO can only transfer the identification of the users, the technical characteristics of the users' communications and the location data.

As the statistics authorities should be considered as being data controllers, the statistics authorities also need to file for a notification as mentioned above and respect all of the obligations provided under the ITLA for data controllers.

As the data will be used for statistical purposes, it would be useful to verify whether the data will be anonymized shortly after being transferred to the statistical authorities. In such a case, the CNIL should be contacted to verify that the anonymization procedure does comply with the ITLA. The MNO would then only need to mention in its agreements with users that their data will be transferred to the statistical authorities. If this is not the case, all of the information indicated in Section 5.1 (Information of the data subjects) above should be provided by the MNO in such agreements.

As an example, the CNIL considered in 2010, that devices analyzing the attendance of certain places (such as airports or commercial centers) by capturing data transmitted by mobile phones and therefore calculating the geographical position of data subjects were compliant with the ITLA if a clear information was displayed in such places on the purpose of the devices and the data controller, and the data was anonymized shortly after being collected by an anonymization process controlled and approved by the CNIL.

In addition, as for Estonia, if the location data is collected to comply with Regulation 692/2011 and the location data is considered as falling under Art 8 (b) of the Regulation 692/2011, the statistical authorities may be considered as acting within the framework of a legal obligation or the performance of a public service mission. In such a case, under Art 6 of the ITLA, consent of the data subject is not necessary for the processing of the location data. As for Estonia, the data will also need to be treated in compliance with Regulation 223/2009.

However, we strongly recommend that the opinion of the CNIL be formally requested on this issue, in particular since location data may not be necessary to provide the information requested under Regulation 692/2011 (in particular pursuant to Art 3 of the Regulation 692/2011) and Art 34-1.V of the PECC, which requests the consent of the data subject for the use of location data, does not provide for any exception in relation to compliance with legal obligations or performance of a public service mission.

Transfer of location data that is personal data to a third party data broker must be conducted on the following terms.

For the purposes of the following analyses we have assumed that the third party data broker would be a data processor and would be situated within the European Union.

The CNIL considers that the following criteria should be taken into account to verify whether a services provider acts as data controller or data processor:

(a) whether the services provider receives general or detailed instructions from the customer,

(b) the level of control exercised by the customer over the services and the data transferred to the services provider (e.g. whether the service provider has a right to use the data as it sees fit),

(c) whether the services provider acts under the customer's name or its own name and/or re-uses the data for its own purposes,

(d) the level of expertise of the services provider (e.g. whether the technical means used to provide the services are imposed by the service provider and cannot be modified by the customer either because the customer does not have the necessary skills or because the software does not require any specific developments).

If the third party data broker is a data processor, we assume that it would act on behalf of the statistical authorities. A data processor is not subject to the obligations provided under the ITLA. However, Art 35 of the ITLA provides that the processor shall offer adequate guarantees to ensure the implementation of the security and confidentiality obligations incumbent upon the controller. This requirement does not exempt the data controller from its obligation to supervise the observance of such measures.

The contract between the processor and the data controller must specify the obligations incumbent upon the processor as regards the protection of the security and confidentiality of the data and provide that the processor may only act upon instructions from the data controller.

If the third party broker is a data processor, consent from the MNO's customers is not necessary for the data to be transferred to it, as the data processor acts under the control of the data controller. A contract between the statistical authorities and the third

party broker will, however, need to be entered into, providing for the obligations mentioned in the preceding paragraph.

8 CONCLUSION AND RECOMMENDATIONS

The above overview lists and introduces the relevant acts on the level of the EU as well as the four sample Member State jurisdictions covered by the Study. Although the EU directives have been transposed and implemented into local laws (with the exception of the DRD not being implemented in Germany as explained above), the implementation practice has proved to be somewhat different resulting in variety of approaches concerning the topic in question. Additionally, the practice applied by regulators in each country, if existing at all, differs to quite some extent.

Based on the above we would like to highlight the following issues.

8.1 *Relevant data*

Conclusion: The data relevant in terms of the Study (refer to Section 7.1) corresponds to the data subject to the data retention obligation under the DRD. It is essential to note that the MNO's obligation to retain data under the DRD does not exempt the MNO from processing personal data according to the general rules of the personal data processing arising from the DPD and the EPD. To further extent the DRD is not relevant in the context of the Study since the obligation to retain data arising thereunder is imposed for the purposes of making data available to law enforcement authorities for the purposes of the investigation, detection and prosecution of serious crime.

8.2 *Location data as personal data*

Conclusion: It is essential to identify whether the data provided by an MNO is deemed personal data. The applicability of the DPD and the relevant local laws depends on whether the mobile positioning data constitutes personal data or not. The DPD does not apply in case the mobile positioning data processed does not qualify as personal data. In such case the data could be freely used, including transferred to the state statistics authorities or third party service providers as may be necessary.

In general personal data means any information relating to a natural person who is or can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Such principle derives from the DPD and is implemented in Member States' local laws with slight differences as to which means one should take into consideration when determining if a person is identifiable or not. In France, for example all the means that the data controller or any other person uses or may have access to should be taken into account. In Germany, means that require a disproportionate amount of time, expense and effort need not be taken into account. However, all in all a conclusion can be drawn that conservative and strict approach is to be taken upon construing the concept of personal data which is why we have concluded the following.

This memorandum is based on the understanding that anonymous data in the context of the Study may in principle be traced down to an identifiable person although such possibilities are limited. We have concluded herein that aggregated data is not subject to the provisions of the DPD and can therefore be processed without limitations arising therefrom. The issue is outstanding in terms of data that is not in aggregated form. Since the qualification of data as personal data comes down to a matter of assessment in each

given situation, there is no universal answer to that question. The laws and the practice in each sample jurisdiction are slightly different. Out of the four sample countries France is the only one where the regulator has provided some guidance as to anonymization keys (refer to Section 5.1 for details). In Finland the Data Protection Ombudsman is currently in the process of preparing a statement addressing the matter in question. Today's guidance on the Working Party level has not addressed the topic at hand in sufficient detail. The general approach of the Working Party is, though, that the mobile positioning data is as a rule personal data. Therefore, if not in aggregated form, it should be presumed that location data is personal data.

Recommendation: Updating and specifying the Working Party guidance would be one option to clarify the issue and achieve unified approach throughout the EU. However, given the differences in transposing the EU directives into local laws and consequent differences in implementation may prevent giving a unified guidance.

As long as the local laws differ, giving further guidance by local regulators (similarly to what the CNIL has given in France) on implementation of the statutory rules is recommended. If guidance on anonymization keys is given, it may, depending on such guidance, occur that in certain cases the anonymized location data is not deemed personal data and the processing thereof is subject to less formalities (e.g. if the anonymization keys are valid for a sufficiently short periods of time, etc.). We also highly recommend consulting the data protection authorities of all relevant EU countries to clarify the accepted practice of applying local laws.

8.3 *Processing location data for official statistics purposes*

Conclusion: If location data is in aggregated form (i.e. cannot be used to single out any individual) it can be processed for statistics purposes without limitation from the data protection perspective. If location data is deemed personal data (i.e. if it not in aggregated form) the approach differs from country to country as to what specific terms and conditions must be met in order for such processing to be lawful.

In France the law requires consent for the processing of location data. Further, it is unclear as to whether compliance with Regulation 692/2011 is considered as a condition which entitles the statistic authorities to collect data without the data subject's consent. Even in such a case, this does not necessarily mean that an MNO would have an obligation to provide this data to the statistic authorities.

In Estonia it is most likely possible to draw a conclusion that personal data may be used for official statistics purposes without the data subject's consent if certain preconditions (as set out above in this memorandum) are met. However, it is unclear if the general basis for processing for the purposes of performing an official task by the statistics authorities would be sufficient to render such processing without the data subject's consent lawful or more specific terms have to be adhered to.

The German law does not currently stipulate the right of the statistics authorities to request relevant data from the MNOs. Such law, if enacted, would have to set forth the detailed terms and conditions of processing the personal data for statistics purposes. However, the Regulation 692/2011, on the preconditions described in Section 7.3 above, would entitle the official statistics producer to claim data from MNOs and process thereof.

In Finland the effective law does not oblige MNOs to provide mobile positioning data to statistics authorities. Therefore there is a need for a mediator that renders the data into

aggregated form on the premises of the MNO but such scenario is challenging technically, financially and in terms of organization.

Therefore, although there are regulations in place on general level in all jurisdictions, the unclarity as to the terms and conditions of processing location data lies in details. In each jurisdiction the principles of the EU directives have been implemented differently. Furthermore, the legal practice and interpretation of the local regulators differ to quite some extent. Therefore the obstacles arising from each relevant jurisdiction are also different.

Recommendation: Although the EU directives serve as the basis for relevant regulation in the Member States, the directives provide for quite some flexibility to the Member States upon transposing the directives into local laws. Consequently, the general unique principles set forth by the EU have been implemented differently in detail in local laws. Thus, in order to obtain a full overview of the obstacles set by local laws, the local laws of all relevant Member States need to be analysed in detail. Due to the variety of issues across the investigated sample jurisdictions (and presuming the jurisdictions not investigated for the purposes of this Study each have their own difficulties of implementation) it is not possible to draw unique and comprehensive conclusions as to how local laws should be amended in order to eliminate all obstacles in processing the location data for statistics purposes. Local laws of each jurisdiction should be reviewed and revised where necessary if no common obligatory guidance is given on the EU level.

One possible solution to eliminate the need to obtain data subject's consent for the processing of personal data for statistics purposes is to verify if the data categories and intended use of the location data in the context of the Study would be covered by those set out in Art 3.1 of Regulation 692/2011 that is directly applicable in all Member States. If not, the list of purposes of use could be modified by a delegated act of the Commission as further described in Section 7.3 above. It is not clear, however, if this would be a viable solution for e.g. in France and Finland although it most likely would be in Estonia and Germany.

Notwithstanding the above, since the practice of interpreting and applying the relevant acts is limited and ambiguous in the investigated countries it is highly recommended to further consult the regulatory authorities in each relevant Member State.

Alternatively, the legislation on the EU level should be amended to be introduced in sufficient detail with more detailed guidance to the Member States for implementation thereof. Given that the Draft Regulation is currently in the process of being negotiated, it would be useful to identify the possibilities of introducing such clarifying provisions in the Draft Regulation that will be directly applicable in the Member States. More specifically, since the delegated acts that the European Commission will be entitled to give under the Draft Regulation will likely be the instruments whereby the specific criteria of processing data for statistics purposes will be set forth, the focus should be on finding ways to highlight the current deficiencies to the Commission and help them draft respective delegated acts so as to introduce the specific enough provisions. That would preclude the need to amend each relevant local law.

Apart from the legislative measures, contractual measures can be applied to overcome the statutory obstacles. The main issue common to all investigated jurisdictions is that either it is not possible to transfer the personal data to statistics authorities without the data subject's prior consent, or it is not fully clear if and on what conditions it may be done. One should bear in mind that obtaining separate consents from data subjects is not practically feasible. Therefore, in each case where the data subject's consent for transfer

of data to by an MNO to the state statistics authorities is needed, it is recommended that the MNOs' agreements with their customers include the customers' respective consent. The consent should not be part of the standard terms and the refusal by a customer to give one should not deprive the customer from entering into the agreement with an MNO. The data subject should be able to revoke the consent at any time. Detailed requirements to the terms and form of the consent should be investigated in each relevant jurisdiction.

8.4 *Transfer of location data to third party data brokers*

Conclusion: The transfer of location data that is personal data to third parties acting as data brokers or in similar function can only be done upon data subject's consent. The only exception to this is the transfer of data to a third party performing an official task as the representative of the state statistics authorities (on the terms and conditions as described in this memorandum). In order for the processing by a third party to be lawful, the relationship between the statistics authorities and such third party should be designed pursuant to the requirements of each local jurisdiction. In Estonia, for example, data brokers should be commissioned with an official task by the statistics authorities under the law or a contract under public law.

Recommendation: In the event third party data brokers are used in the model of processing the location data for statistics purposes, and provided that the conditions to the lawful processing by the statistics authorities are met in each relevant jurisdiction, it is necessary to identify what type of legal relationship needs to be created between the statistics authorities and the data broker in each relevant Member State jurisdiction.

Sincerely yours,

Attorneys at Law Borenius