Õiguskantsler

Mr Urmas Reinsalu
Ministry of Justice
info@just.ee

Your ref.

Our ref. 20.07.2015 No 6-1/140621/1503191

Opinion of the Chancellor of Justice

Dear Minister,

On 15 July 2014 Chancellor of Justice Indrek Teder contacted the Minister of Justice with a request for information that concerned the issue of the constitutionality of the retention and further processing of electronic communications data stipulated in § 111^1 of the Electronic Communications Act (hereinafter ECA).

In its letter, the Minister promised to answer the questions of the Chancellor of Justice and carry out a comprehensive analysis of the constitutionality of the regulation of preventive collection of electronic communications data by the end of 2014. On 29 December 2014 the Deputy Secretary General for Legislative Policy informed us that carrying out the analysis would take more time than initially thought and that the results would be sent to the Chancellor of Justice as soon as possible.

Considering the long duration of the proceedings, the Chancellor of Justice considered it possible to give to the applicant a partial answer about the constitutionality of § 111^1 of the ECA without awaiting your opinions. The Chancellor of Justice hereby also sends her opinion to you.

Opinion of the Chancellor of Justice about the constitutionality of § 111^1 of the Electronic Communications Act

1. Introduction

The petitioner contacted the Chancellor of Justice and requested a review of the constitutionality of § 111^1 of the ECA. In its opinion, the applicant referred to Judgment of the European Court of Justice in joined Cases C-293/12 and C-594/12 of 8 April 2014 (hereinafter the ECJ judgment). In said case, the European Court of Justice (hereinafter the ECJ) decided that 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 Directive 2006/24/EC) is incompatible with Articles 7, 8 and 52 (1) of the Charter of Fundamental Rights of the European Union (CFREU), and annulled it. The applicant therefore argued that the constitutionality of § 111^1 of the ECA, established for the national implementation of said directive, is also doubtful.

Since the petition was connected to the conclusions arising from the ECJ judgment, it must first be emphasised that the opinions given in said judgment only concern the directive and cannot be directly extended to the national legislation established for the implementation of the directive.

Also, the conclusion made about the directive cannot be directly transferred to our legal order for the reason that the latter only stipulated framework requirements in many issues and left EU Member States a broad margin of discretion in furnishing them. In many issues, the regulation of the ECA goes further than the directive and the minimum requirements stipulated therein.

The invalidity of the directive does therefore not allow for drawing conclusions that the national regulation issued on the basis thereof is in any case unconstitutional and must therefore be annulled, not to mention its automatic invalidity.

However, there is no doubt that the opinions of the ECJ about the rights arising from the CFREU must be used as interpretation arguments in furnishing the provisions of the Constitution. It must also be kept in mind that the majority of the principles highlighted by the ECJ in the judgment are not specific principles of EU law, but are based on the case law of the European Court of Human Rights (ECtHR) in furnishing the European Convention on Human Rights (ECHR) (the ECJ has referred to the case law of the ECtHR by way of analogy in many cases), as well as the generally recognised principles of democratic states governed by the rule of law in the protection of fundamental rights.

It can also be pointed out that the Criminal Chamber of the Supreme Court has assessed the constitutionality of said regulation in its judgment of 23 February 2015 in Case No 3-1-31-51-14 in the part that concerns the collection and retention of communications data when a criminal procedure is being conducted, and found that the regulation is constitutional (see p 22 of the judgment). Since this is an opinion given within the scope of a specific review of provisions (e.g. proceeding from a specific case), which proceeds from the Code of Criminal Procedure effective before 1 January 2013 in conjunction with the provisions of the ECA, the conclusions made therein cannot be extended to the whole ECA and the preventive data back-up regulation of related other laws *de lege lata*. Still, the opinion given in the judgment has a significant meaning also from the viewpoint of this analysis and the conclusions made have been used for the purposes of criminal procedure in regard to data processing.

The following must be noted about the scope of the analysis. This is an abstract assessment of provisions within the scope of which the Chancellor of Justice considers it necessary to distinguish between two sides. As seen below (see p 1), the assessment of constitutionality in this case cannot be restricted to the isolated analysis of a section of the ECA, as the legal institute in question consists of several parts and covers a number of different procedures and legal issues. Considering the large scope of the procedure and the fact that the Chancellor of Justice has not yet received the responses of the executive authorities to the questions presented upon the initiation of this procedure[1], the Chancellor of Justice considers it possible to only assess the constitutionality of the communications data processing in the part that concerns the collection and retention of data by the communications operators. However, it is impossible to provide a final opinion of the regulation that concerns the constitutionality of the fact that public authorities demand communications data and process them further (incl. adequacy of procedural guarantees). It must be said that both parts of said analyses are connected to each other and certainly influence one

[1] The Chancellor of Justice sent a letter to the Minister of Justice, the Minister of the Interior and the Minister of Economic Affairs and Communications on 15 July 2014.

another, but division is still possible in the opinion of the Chancellor of Justice. The Chancellor of Justice will send the remaining part of the analysis to you as soon as possible.

2. Assessed legal regulation and infringed fundamental rights

You asked the Chancellor of Justice to check the constitutionality of § 111^1 of the ECA. Subsections (2) and (3) of said paragraph set forth the communications operator's obligation to retain the listed electronic communications data. The remaining subsections of the paragraph determine the terms and conditions of data retention, incl. the general retention term of over one year (subsection (4)), the requirements for guaranteeing data security (subsection (9)), and the basis of transmitting data to public authorities (subsection (11)).

Although § 111^1 of the ECA contains the core of preventive data back-ups, a comprehensive assessment of the constitutionality of the retention and processing of electronic communications data must consider the fact that the terms and conditions of processing data that is subject to retention are also determined by the other provisions of the ECA and of other acts in conjunction with this. The terms and conditions of communications data to be retained are also regulated by §§ 112, 112^1 and 114^1 of the ECA, and the general provisions in §§ 101 *et seq* of the ECA that regulate the protection of electronic communications data. Transmitting the data retained on the basis of § 111^1 of the ECA to public authorities and further processing of such data is regulated by the provisions of the Code of Criminal Procedure, the Code of Misdemeanour Procedure, the Security Authorities Act and the other acts listed in subsection 111^1 (11) of the ECA. It is therefore necessary to consider the other provisions that regulate the institute of data retention and further processing in conjunction with each other.

The legal institute in question covers a large number of different activities with electronic communications data. The main stages that can be distinguished are collection of electronic communications data, data retention by the communications operator, transmission of the data to competent authorities at the request of the latter, and further processing of the data by the competent authority. This means that the nature and intensity of the infringements of fundamental rights that arise from the measure in its different stages may be different. Whilst the rights of all data subjects are infringed in the same manner and with the same intensity upon the primary collection and retention of information by the communications operator, then the intensity of the infringement varies when data is transmitted at the request of a competent authority and then processed depending on the quantity in which and the length of the period for which data are submitted, the basis on which this is done, i.e. the procedure within the scope of which they are processed (criminal procedure, misdemeanour procedure, administrative procedure), what the procedural guarantees effective in this procedure are, appeal options, etc.

The data mentioned in subsections 111^1 (2) and (3) of the ECA are technical data about the electronic communications sessions carried out by individuals. Such data can be regarded as personal data that describe a person's activities in the electronic communications network in giving and exchanging data.

The first sentence of § 26 of the Constitution stipulates that everyone is entitled to the inviolability of his or her private and family life. Protection of private life as a whole arises as a general provision from said provision, which also protects the right to informational self-determination, incl. the right to decide about the processing of one's personal data by the public authority. This means that there is no doubt that the collection and further processing of personal data in the manner set forth in § 111^1 of the ECA infringes the area protected by the inviolability of private

and family life. The Supreme Court also came to the same conclusion in its judgment in Case No 3-1-1-51-14 (see p 22 of the judgment).

§ 111^1 of the ECA does not prescribe the collection and further processing of data that concerns the content of the messages transmitted in electronic information channels. Subsection (9) 4) of said paragraph expressly requires communications operators to guarantee that any data concerning the content of communications is not retained. This means that in this case, data processing does not violate the confidentiality of messages transmitted by commonly used means that arises from the first sentence of § 43 of the Constitution.

The statement made in the ECJ judgment (p 28) that the processing of communications data in the manner set forth in § 111^1 of the ECA may influence, direct and restrict the behaviour of persons in the use of means of communications must be agreed with. This means that it cannot be precluded that there will be no negative influence on the right to freedom of speech set forth in subsection 45 (1) of the Constitution or area protected by the right to freedom of self-realisation arising from § 19 of the Constitution via data processing on the basis of § 111^1 of the ECA. However, this is not a case of the direct and purposeful influencing of these rights by the public authority, but of a possible consequence whose intensity in the opinion of the Chancellor of Justice is not great enough to require a separate analysis of the constitutionality of the infringements of the areas of protection of such fundamental rights.

3. Conditions of constitutionality of an infringement

The assessment of the constitutionality of an infringement takes place at the formal and material levels of constitutionality. In this case, the Chancellor of Justice sees no need to assess the formal constitutionality of the infringement, as there is no doubt that the provisions in question were established within the scope of correct legislative procedure and comply with the other formal conditions of an infringement, incl. being legally clear in the main issues.

Assessing the material constitutionality of the freedom of private life requires the identification of the legitimate objective of the infringement, placing this objective under permitted limitations and assessment of proportionality in terms of suitability, necessity and moderateness.

3.1. Legitimate objective of infringement

The right to the inviolability of family and private life is a fundamental right with a qualified reservation of law, which pursuant to the second sentence of § 26 of the Constitution in the cases provided for by law can be restricted to protect public health, public morality, public order or the rights and freedoms of others, to prevent a criminal offence, or to apprehend the offender.

The regulation, which requires data retention and transmission of the data, was introduced to the ECA in order to adopt the directive (Explanatory Memorandum to the Draft Act for Amendment of the ECA and Public Health Act, page 2 *et seq*), which is why the objectives attributed to the directive can be considered the objectives for which the regulation was implemented. The objective of the directive according to its preamble was to harmonise the law of Member States for the investigation, detection and prosecution of serious crimes defined in their national law (Article 1 (1) of the directive). Thus, the main objective of the directive in general terms was to help fight serious crime and thereby protect public security. The explanatory memorandum to the draft also confirms that these are the observed objectives (page 10), and states that the ultimate

goals of backing up electronic communications data is to fight terrorism and guarantee internal security.

There is no doubt that the objective of the investigation, detection and prosecution of serious crimes can be placed on the limitation reasons of prevention of a crime and apprehension of an offender (the Supreme Court found the same in p 22 of the judgment in Case No 3-1-1-51-14). On a broader scale, the prevention and prosecution of serious crimes also serves the purpose of guaranteeing public order and the rights and freedoms of other people.

However, the ECA stipulates the use of retained data for considerably broader goals than the direct prevention and prosecution of serious crimes intended with the directive. Clause 111^1 (11) 1) of the ECA does not differentiate between crimes according to their seriousness, but allows data to be transmitted for the prosecution of any crime if all other requirements for requesting data have been met. Clauses 111^1 (11) 2) to 6) of the ECA also require communications operators to transmit retained data to competent authorities for the guaranteeing of security, the processing of misdemeanours, financial supervision, decisions in civil court procedures and so-called background checks of persons by surveillance authorities.

The Chancellor of Justice is of the opinion that the objectives of the regulation that are not connected to the prosecution of crimes can also be covered by the limitation reason of the protection of public order and the rights and freedoms of other people for the purposes of § 26 of the Constitution. The activity of surveillance authorities in the performance of duties outside criminal procedures that arise from the Surveillance Authorities Act are also covered by the objective of crime prevention.

However, even if it were possible to claim that some of the aforementioned objectives cannot be placed within the framework of qualified limitation reasons, the legitimacy of one of the listed objectives would be enough for guaranteeing the legitimate objective of data retention. There is no doubt that the investigation, detection and prosecution of serious crimes is such a goal.

3.2. Proportionality of infringement

3.2.1. Suitability

The collection and retention of electronic communications data by communications operators is an unavoidable premise for competent authorities to be able to access such data during a certain period of time and perform their duties. The preservation of communications data creates preconditions for the achievement of objectives that, considering the importance and share of electronic data communication, could not be achieved without data retention or the achievement of which would be considerably more difficult. Collection and retention of data by communications operators can be considered a suitable measure when it facilitates the achievement of just one of the objectives listed above. There is no doubt that the retention of data and the possibility to use them later on helps to carry out criminal procedures - the Supreme Court also confirmed this (p 22 of judgment in Case No 3-1-1-51-14). It is therefore a measure suitable for the achievement of objectives.

3.2.2. Necessity

The Chancellor of Justice is of the opinion that it is impossible to refer to any specific measures that would clearly be as effective in the achievement of the objective of the infringement as the collection and retention of communications data to the extent and in the manner set forth in § 111^1 of the ECA. It would be possible to collect less data and in respect of a smaller group of persons, or to retain the data for a shorter period of time, but the effectiveness of the measure would presumably decrease in such a case, because the state would have at its disposal less data on the basis of which to fight crime or achieve the other aforementioned objectives. The Supreme Court also confirmed that data retention is a necessary means for the detection and prosecution of crimes, starting that "this is an effective measure for obtaining objective proof of the fact that persons communicated and where they were, the collection of which in any other manner is not certain or guaranteed" (see p 22 of judgment in Case No 3-1-1-51-14).

3.2.3. Moderateness

In this case the assessment of the constitutionality of a regulation lies in the assessment of the moderateness of the infringement. In other words, it is important whether the infringement of the freedom of private life arising from the collection and retention of data is sufficiently balanced by the objective of the measure to protect the aforementioned constitutional values and with the procedural guarantees and other conditions limiting the infringement.

Both the Supreme Court and the ECtHR have emphasised the dependence of the constitutional permissibility of infringements on the freedom of private life on the existence of sufficient legal conditions that limit infringement, procedural guarantees and an efficient supervision system, whereas the guarantees must be more effective the more intense the infringement of a fundamental right is (e.g. about the limitation of the freedom of private life in the context of surveillance: Supreme Court judgment of 20.03.2014 in Case No 3-4-1-42-13, p 57 and 74; ECtHR judgment in the Case S and Marper vs United Kingdom, p 99).

The infringement of the inviolability of private life under § 111^1 of the ECA can be considered rather serious at the level of data retention alone. Although the retained data do not cover the content of the transmitted messages, the large quantity of retained data and the extensive role of electronic communications in the relationships of people certainly allows for conclusions to be drawn about the private lives of persons, their habits, interests, circle of communication and so on. As the importance of electronic communications increases in relationships between people, the quantity of data that can be obtained about a person also increases, as does the possible intensity of the infringement.

The intensity of the infringement is also increased by the fact that data are automatically collected and retained, and prescribed for all generally used means of communication (telephone, mobile phone, Internet, Internet telephone) and all communications sessions that have taken place without being in any way whatsoever dependent on the lawfulness or unlawfulness of the communicating person, the geographic region in which and the time at which communication takes place, or other conditions. This means that the measure is also an infringement of the rights of persons in respect of whom there is no need to collect and retain data in light of the measure's aforementioned objectives, and the transmission of whose data on the basis provided for by § 111^1 of the ECA is never actually necessary. The data subject themselves is completely unable to have any impact through their behaviour on whether or not data is retained about them.

Although data retention and transmission do not constitute surveillance, the automatic and non-selective retention of all data may create a feeling of being watched in society. Although persons know which data about their communications sessions is retained and for how long, it is impossible for them to directly control the conditions of data retention or who can access such data.

There is no doubt that the permanent retention of large quantities of data by communications operators carries a risk of offences and unlawful use or publication of the data, irrespective of the security measures that have been taken.

On the other hand, it is also necessary to consider the significance of the objectives of the infringement and the protected benefits. There is no need to explain that the constant increase in the use of electronic communications in society has turned it into a tool used to commit offences, disturb public order or damage the rights and freedoms of other people in another manner. The threat that electronic communications are used to commit serious crimes like terrorism or other organised crime is particularly serious, and fighting this has been the main objective of the directive and the ECA regulation issued on the basis thereof.

The right of organisation and procedure, and the fundamental right of protection, which require the state to guarantee the exercise and protection of the fundamental rights of people with sufficient probability and to a sufficient extent via its factual and normative activities, arise from both the Constitution and the ECHR (e.g. Supreme Court en banc, judgment of 16.05.2008 in Case No 3-1-1-86-07, p 23; Constitutional Review Chamber, judgment of 20.03.2014 in Case No 3-4-1-42-13, p 44).These obligations of the state must, among other things, be interpreted as changing over time; the state must adapt to the new situation in guaranteeing internal peace, incl. the continuing increase in the importance of electronic communications and the need to prevent and prosecute offences and other violations of law also by using information technology means and the information obtained from the electronic environment.

It is thereby important that access to communications data does not just facilitate the performance of the state's duties, but the various facts of importance in the protection of rights can actually be identified due to the increased importance of electronic communication only by gaining access to certain communications data.

In its judgment (p 56-59), the ECJ also argues that in order to guarantee the necessity of the measure, the directive should not have stipulated the automatic retention of the data of all persons, but limited the data to be retained on the basis of geographic, personal, temporal or other characteristics in such a manner that the specific retained data had a connection to the fight against serious crime set as the objective of the directive. The ECJ found that the directive did not border on unavoidably necessary infringement in this respect.

Similar to the provisions of the directive, § 111^1 of the ECA also stipulates the general retention of data in respect of all communications sessions and all persons.

Irrespective of the opinion of the ECJ, the Chancellor of Justice feels it is unclear how and based on what criteria it would be possible to retain communications data selectively in such a manner that it guaranteed effective protection of the rights and freedoms of persons in the information society, especially the prevention and prosecution of serious crimes. Considering the general unpredictability of people's activities, which in the case of criminals is also characterised by their desire to conceal their intentions and actions, there is reason to doubt whether and to what extent it is possible to select an activity that is potentially aimed at the commission of an offence or other

violation of law before or during a communications session. Even if limiting criteria were thinkable, they would in any case increase (provided that they were established by law and were public) the possibility to conceal the commission of crimes or evade the requirement of retention. Even if such selection were possible to some extent and released some of the persons who use communications service from the infringement of their freedom of private life, it might call for the more extensive use of other, considerably more intensive measures that infringe fundamental rights in order to guarantee the efficiency of the fight against serious crime, e.g. the application of surveillance if there were no way of obtaining the necessary data with less infringing measures.

The establishment of selection criteria would also fail to guarantee that personal data were only collected for persons in the case of whom further processing of data was unavoidably necessary for the achievement of the goals of criminal procedure or the other objectives listed in subsection 111^1 (11) of the ECA, i.e. there would be no justification based on specific procedural goals for the collection and retention of the data of some persons' communications data also in the future. The establishment of selection criteria would bring about the threat of arbitrary conduct and the unjustifiable unequal treatment of persons.

It must also be taken into account that the intensity of an infringement is reduced by its limitation to the technical data of communications alone, and the fact that the content of messages is not reflected among the recorded data. Even if the infringement may cause a certain fear of being watched in society, its general and balancing preventive influence cannot be denied either, as it discourages the commission of crimes and other violations of law, as the person realises that they can later be ascertained.

In p 22.3 of its judgment in Case No 3-1-1-51-14, the Supreme Court pointed out that the need to collect and retain the data listed in § 111^1 of the ECA (or at least some of them) exists independently of the need to process them for public law goals. The correctness of this conclusion was confirmed by communications operators at their meeting with the Chancellor of Justice. Namely, communications operators had the legal right to retain the communications data of their customers for business (contractual) purposes even before the establishment of § 111^1 of the ECA. The effective § 104 of the ECA also gives communications operators the right to process the data concerning the provision of communications services without the consent of the customer if this is necessary for submitting bills to the customer, incl. determination and calculation of interconnection charges. Subsection 106 (2) of the ECA states that said data can be retained for up to 1 year from payment for the communications service. This fact as such does not provide a separate reason for the retention of communications data for public law objectives, but it demonstrates that an infringement of similar content existed and exists in the provision of communications services due to their essence alongside the relevant risks of misuse and other threats generated by the retention of data. The Supreme Court has also noted that communications operators could have been ordered to provide the data retained for private law purposes in criminal procedure even before the establishment of § 111^1 of the ECA.

Procedural guarantees and other defining conditions are important in the assessment of the moderateness of an infringement.

The types of data to be retained have been clearly and exhaustively stipulated, and subsection 111^1 (4) of the ECA establishes the obligation to obtain communications data for one year after it took place. The Government of the Republic can make exceptions to this rule in the interests of public order and security. The retained data must immediately be deleted when the retention term ends (subsection 106 (3) of the ECA). The Supreme Court assessed the moderateness of the one-year

term (in the context of criminal procedure) in p 22.3 of its judgment in Case No 3-1-1-51-14, and found that this term was not excessively long.

Subsection 111^1 (5) of the ECA requires the retention of data in the territories of European Union Member States to guarantee a uniform control and data protection standard.

Subsection 111^1 (9) of the ECA stipulates the obligations of communications operators to guarantee data security with the following measures:
1) compliance with the same quality, security and data protection requirements that are applied to other similar data in the electronic communications network;
2) protection of data from accidental or unlawful destruction, loss or amendment, unauthorised or illegal retention, processing, access or publication;
3) necessary technical and organisational measures for restricting access to data;
4) guaranteeing that any data concerning the content of communications is not retained.

Although said obligations are rather generally expressed, it is clear that data protection must be guaranteed at least at the same level of protection that is applied to other similar data processed by the communications operator. The obligations of communications operators and requirements for processing the personal data of customers under the Personal Data Protection Act and the ECA also apply to the protection of the retained data (see §§ 102 and 102^1 of the ECA). Among others, a communications operator is also required to inform the Data Protection Inspectorate of any violations related to personal data as soon as possible (subsection 102^1 (2)) and also to inform a customer or other person in the event that the inviolability of their personal data and personal life has been breached. Communications operators are also obliged to keep account of violations related to personal data. Subsection 106 (1) limits the circle of persons entitled to process the retained data with the communications service provider and the persons authorised by the latter.

The representatives of companies that provide large volumes of communications services (mobile operators) interviewed by the Chancellor of Justice claimed that they have separated the data specified in § 111^1 of the ECA from the other data generated upon the provision of communications services as a separate set of data, access to which is internally restricted and controlled. However, it is still unclear whether such additional guarantees to the inviolability of data are applied by all service providers, as the ECA does not expressly stipulate such an obligation.

No separate supervision mechanism has been prescribed in respect of data collection and retention, but the supervision competence of the Data Protection Inspectorate extends to the collection and retention of personal data according to the Personal Data Protection Act and subsection 133 (4) of the ECA. The general competence of state supervision in the area of electronic communications lies with the Technical Regulatory Authority, which among other things collects data from communications operators about the data retained on the basis of § 112^1 of the ECA. The law gives law enforcement authorities the option of implementing administrative coercive measures when exercising state supervision. § 42 of the Personal Data Protection Act also provides the option of imposing misdemeanour punishment for failure to apply personal data protection measures or other requirements of personal data processing. In terms of penal law, punishment for unlawful disclosure of personal data in professional or official activities is also guaranteed.

In conclusion, the Chancellor of Justice is of the opinion that the infringement of constitutional rights arising solely from the collection and retention of data by communications operators cannot be considered overly intensive for the user of communications services. Although the data of all

communications service providers and communications sessions are retained, the retained information does not contain the content of messages and is balanced with the objective need to guarantee the fight against crime and protection of public order and people's rights and freedoms in a situation that considers modern technology, where there are usually no reasonable alternatives for obtaining such data.

The threat to the rights of the data subject in this stage of infringement proceeds primarily from the possible unlawful use or disclosure of their data by the communications operator or another person who has managed to access data, which is something that must be prevented by the aforementioned procedural guarantees, supervision and options for contesting.

The objective of the ECA is not to establish a data protection standard for the retained data that in its essence is higher in comparison to similar data in the electronic communications network, thereby proceeding from the general personal data protection requirements. The requirements for data security and lawful processing are also stipulated in subsection 111^1 (9) of the ECA rather as the objectives of the activities of communications operators in guaranteeing data protection, and the ECA does not present any specific measures that must be taken to guarantee data security. Effective law does not stipulate the obligation to create a special mechanism for checking the security of such data, special dispute procedures in case of suspicions that rights have been violated and so on.

Irrespective of this, the Chancellor of Justice does not consider it possible to take the position that the obligation to comply with the general requirements of personal data protection concerning equally important information that are effective in the area of electronic communications, which is connected to the option of implementing state supervision and punishment for misdemeanours, does not guarantee compliance with the requirements set forth in the Constitution in every case. It is difficult to derive from the Constitution which specific requirements (with which compliance is not required by effective law) should in any case apply to the retention of the data stipulated in § 111^1 of the ECA in comparison to the retention of other personal data of customers. Although the case law of the ECtHR also refers to the need to ensure the necessary guarantees against misuse upon personal data processing, and it is considered particularly important in cases where data is automatically processed (e.g. in the case of S and Marper vs United Kingdom, p 103; M.K *vs* France, p 30 et seq), it is impossible to point out any specific guarantees that are fully missing and the existence of which would be required in this context. The Chancellor of Justice is therefore of the opinion that the regulation of preventive collection and retention of data, as set forth in § 111^1 of the ECA, is not clearly immoderate and therefore is not in contravention of the Constitution.

4. Summary

In conclusion, the Chancellor of Justice is of the opinion that the abstract analysis of constitutionality does not make it possible to conclude that § 111^1 of the ECA is in contravention of the Constitution in the part where it prescribes the automatic collection and retention of electronic communications data by communications operators for a term of one year. The Chancellor of Justice admits that the provisions governing data collection and retention are not perfect, but does not consider it possible to conclude that this has caused an unconstitutional situation.

As stated above, the Chancellor of Justice does not take a position about the constitutionality of the further processing of communications data (incl. the procedural guarantees and other conditions that limit infringement upon data processing) by public authorities. However, the

Chancellor of Justice still says that should she identify the unconstitutionality of the further processing of data in subsequent analysis, it may in her opinion have an impact on her opinion of the regulation of preventive backing up of data as a whole.

The Chancellor of Justice also considers it necessary for the executive power (if necessary, in cooperation with various ministries, the Data Protection Inspectorate, the Technical Regulatory Authority and other authorities) to additionally assess and analyse issues related the adequacy of procedural guarantees in the process of data collection and retention by communications operators. It is certainly important to also assess the present practices of communications service providers in the performance of their obligations, possible cases of unlawful use of data or other misuses, etc.

The Chancellor of Justice is of the opinion that is should also cover consideration of the need to

- stipulate more specific requirements for the obligations of communications operators upon data retention than those in the effective subsection 111^1 (9) of the ECA, incl. upon the separation of communications data from other data into data sets subject to enhanced security requirements and a more specific definition of the persons who have access to them, as well as specification of the procedure for destruction of the data;
- stipulate a separate supervision mechanism or requirements for the retention of communications data.

Yours sincerely,

/digitally signed/

Ülle Madise

Mait Laaring 6938432
Mait.Laaring@oiguskantsler.ee