Decision 15/2022 (VII. 14.) AB

on establishing a violation of the Fundamental Law by an omission related to the regulation under section 157 (2), (3) and (10) and section 159/A of the Act C of 2003 on Electronic Communications

The plenary session of the Constitutional Court, in the subject of a constitutional complaint – with concurring reasonings by Justices dr. Ágnes Czine and dr. Zoltán Márki – adopted the following

decision:

1. The Constitutional Court, acting *ex officio*, finds that the Parliament had caused an infringement of the Fundamental Law by its failure to act in accordance with section 157 (2), (3) and (10) and section 159/A of the Act C of 2003 on Electronic Communications, which is not in line with the constitutional requirements of the right to privacy under paragraph (1) and the right to the protection of personal data enshrined in paragraph (3) of Article VI of the Fundamental Law.

The Constitutional Court, therefore, calls upon the Parliament to comply with its legislative duty by 31 December 2022.

2. The Constitutional Court rejects the petition seeking the declaration of section 159/A of the Act C of 2003 on Electronic Communications being in conflict with the Fundamental Law and its annulment.

The Constitutional Court orders the publication of its decision in the Hungarian Official Gazette.

Reasoning

I

[1] 1 The petitioner, through its legal representative (Dr. Tivadar Hüttl, attorney-at-law), filed a constitutional complaint pursuant to section 26 (1) of the ACC against section 159/A of the Act C of 2003 on Electronic Communications (hereinafter: AEC) as the basis of the judgement No. 8.Pf.21.057/2015/5 of the Budapest-Capital Regional Court

of Appeal as the court of second instance.

The petitioner sought a declaration that the said provision was contrary to the Fundamental Law and annulment of the said provision and a declaration of its prohibition of application in the case in question.

[2] 2 On 11 April 2014, the petitioner submitted a request to his electronic communications service provider (hereinafter referred to as the "Service Provider") to disclose to him personal data concerning the petitioner and specified in in points (a), (b), (d), (e), (f), (g) and (k) of paragraph (1) of section 159/A and in section 159/A (2) of the AEC, at the same time to delete them and to inform him of the persons who have been granted access to such data, as well as the data received or obtained by the bodies and persons who have access to such data and the purposes of such data access. In its letter of 14 May 2014, the Service Provider concerned partially provided the requested information, but refused to delete the stored data, as it is obliged under the law to keep them pursuant to section 159/A of the AEC.

[3] The petitioner applied to the court for a declaration that his right to the protection of personal data had been infringed. On 27 November 2014, the Budapest-Capital Regional Court acting on first instance initiated a specific review procedure by the Constitutional Court, which was rejected by the Constitutional Court by the ruling 3082/2015 (V.8.) AB (hereinafter: CCRul.), on the grounds that "in the case under review [...] it is not the provision challenged by the judge that prevents the plaintiff's request from being granted, but other provisions of the AEC, and the related provisions of the FOIA" (CCRul., Reasoning [23]), and the court failed to initiate the examination of these provisions of the law.

[4] The Service Provider provided additional information during the court proceedings at first instance, as a result of which the petitioner maintained his claim in respect of the deletion of personal data. The court of first instance dismissed the action, basing its judgement No. 68.P.21.990/2015/3, inter alia, on section 159/A (1) (a) to (k), (2), (3) and (4) of the AEC. According to the court, the personal data were processed by the defendant on the basis of a statutory provision and therefore the petitioner could not request their deletion.

[5] Following the petitioner's appeal, the Budapest-Capital Regional Court of Appeal, in its judgement of 7 April 2016, No 8.Pf.21.057/2015/5, upheld the judgement of the first instance, on the ground that section 159/A of the AEC provides for mandatory data processing, and therefore the petitioner may not request the deletion of his personal data.

[6] 3 In his constitutional complaint, the petitioner argued that section 159/A (1) (a) to (k) and (2) of the AEC violated his right to respect for privacy and the protection of his personal data, as guaranteed by Article VI (1) and (2) of the Fundamental Law.

[7] According to the petitioner, neither section 159/A of the AEC nor any other statutory rule governing the application of that section contains clear and precise limitations on the general and unlimited nature of data retention. Thus, the legislative provision in question restricts the petitioner's right to respect for privacy and to the protection of personal data guaranteed by Article VI of the Fundamental Law.

[8] According to the arguments put forward by the applicant, such a restriction of fundamental rights is not strictly necessary and is not proportionate to the aim pursued and therefore infringes the requirements laid down in Article I (3) of the Fundamental Law, that is to say, it is contrary to the Fundamental Law.

[9] The petitioner explained that the restriction of the fundamental right was laid down in an Act of Parliament and that there is no doubt that the purpose of the restriction of the fundamental right can be regarded as legitimate, since the retention of data serves the purposes of law enforcement, national security and national defence as constitutional values. The appropriateness of the restriction of rights cannot be disputed in principle, since the data retained under section 159/A of the AEC cover a large part of the means and channels used nowadays for everyday communication, thus there is no doubt that the knowledge of traffic data of the communication means and channels concerned may be suitable for increasing the effectiveness of law enforcement and national security.

[10] However, in the petitioner's view, the stockpiling of data provided for by the contested provision does restrict the fundamental rights concerned not to the extent strictly necessary. On the one hand, to justify the obligation to retain data, the justification for the restriction of the fundamental right with reference to the prosecution of serious crimes does not satisfy the criterion of absolute necessity, since the term “serious crime” does not describe with sufficient precision the crimes for which the mandatory data processing is carried out. The obligation of data retention (and transfer) under section 159/A of the AEC is not limited to cases where the restriction of rights would be truly indispensable. On the other hand, the scope of the data retention obligation applies to all subscribers, users and persons who come into contact with them in general, without them being in a situation that could give rise to criminal proceedings or pose a threat of terrorism or national security, even indirectly. Furthermore, it applies not only to individuals but also to means of communication and to the data as a whole in general, without any temporal, geographical or personal distinction, limitation or exception based on the law enforcement, national security or defence purposes of the processing.

[11] The petitioner also holds that the restriction is also not proportionate to the aim pursued. On the one hand, because the rules on access and subsequent use of retained data do not contain objective criteria – substantive and procedural conditions – that public authorities would have to justify in order to access and use the data (thus to seriously interfering with a fundamental right). The disproportionality is further aggravated by the fact that access to data is not subject to prior review by an independent body. On the other hand, there is also a lack in the regulation of safeguards to ensure the participation of the applicant (right to information, right to object, right to rectification, right to erasure) and to enforce his rights.

[12] 4 In connection with their legal position and practice in relation to the petition, the Constitutional Court contacted the Ministry of the Interior, the Ministry of Justice, the National Authority for Data Protection and Freedom of Information (hereinafter: NAIH), and the service providers subject to the data retention obligation, pursuant to section 159/A of the AEC, as electronic communications service providers licensed in Hungary. The Constitutional Court has taken account in the course of its proceedings of the observations made in the opinions sent in reply to the requests.

[13] 5 The Constitutional Court admitted the constitutional complaint at its session of 11 July 2017, because the question of whether the general, unconditional and "stockpiling" data processing provided for in the challenged statutory provisions violates the fundamental rights to privacy and the protection of personal data under Article VI of the Fundamental Law is of fundamental constitutional importance.

II

[14] 1 The affected provisions in force of Fundamental Law at the time of submitting the petition:

"Article VI (1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected.

(2) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest."

[15] 2 The challenged provisions of the AEC in force at the time of examining the petition:

"Section 157 (1) After the provision of an electronic communications service, the electronic communications service provider shall, except as provided for in paragraph (2) and paragraph (1) of section 159/A, delete or anonymise personal data relating to subscribers and users which it processes in the course of providing the service.

(2) The electronic communications service provider shall process the following data generated in the course of billing the subscriber and collecting the related fees and monitoring subscriber contracts in order to fulfil its statutory duties, to provide data upon request, and in connection with the provision of the subscriber service, where this is reasonable for the subscriber concerned, in the performance of the statutory duties of the court, prosecutor's office, investigative authority, body conducting preparatory proceedings, administrative body and national security service entitled to request data:

(a) the data referred to in points (a) to (e) of paragraph (2) of section 154;

(b) the number or other identifier of the subscriber station;

(c) the address of the subscriber access point and the type of the station;

(d) the total number of units that may be accounted for in the accounting period;

(e) the calling and called subscriber numbers;

(f) the type, direction, starting time and duration of the call or other service and the amount of data transmitted, the network and cell providing the service and the unique identifier of the equipment used to receive the service (IMEI) in the case of mobile radio telephony services, and the identifiers used in the case of IP networks;

(g) the date of the call or other service;

(h) data relating to the payment of charges and the amount of charges due;

(i) the events of termination of the subscriber contract in the event of non-payment;

(j) in the case of telephone services, data relating to other non-electronic communications services which subscribers and users may use, in particular the billing thereof;

(k) data relating to the use or attempted use of subscriber terminal equipment in the electronic communications network of the provider which has been used unlawfully to provide the subscriber service, in particular by the owner of the equipment, including any disconnection of such equipment.

(2a) The service provider shall process the data referred to in paragraph (2) for the purpose of billing the subscriber and collecting the related fees, as well as for the purpose of monitoring subscriber contracts within the limitation period pursuant to paragraph (2) of section 143.

(3) The service provider shall process the data referred to in paragraph (2) (a) for the purpose of fulfilling the data requests of the bodies specified in paragraph (2) in connection with the performance of their statutory tasks, exclusively until the end of the retention period pursuant to section 159/A (3).

(4) The electronic communications service provider may process the data referred to in paragraph (2) for the purpose of providing value-added services or for its own commercial purposes, with the express prior consent of the subscriber or user, to the extent and for the duration necessary for the provision or sale of such services. The electronic communications service provider shall ensure that the subscriber and the user may withdraw their consent at any time.

(5)

(6) The electronic communications service provider shall separate the processing of data for the various purposes permitted or required by this Act or other laws. The separation may be made

(a) in physically separate processing systems according to the purpose of processing, in which the data that can be processed for different purposes are stored independently of each other;

(b) a logically separate processing system, where data that can be processed for different purposes are stored in a common system, but access to the data is separated according to the purpose of the processing.

(7)

(8) Among the data referred to in paragraph (2), the subscriber's name and surname, name at birth, place of residence, information on his/her place of residence, subscriber station number or other identifier, the subscriber numbers calling him/her and the subscriber numbers called by him/her, the date and time of the call or other service, the date and time of the start of the call or other service may be disclosed to the National Bank of Hungary proceeding in its role in the supervision of the financial intermediary system in the context of proceedings for the supervision of compliance with the rules on insider dealing, market manipulation, unauthorised provision of services, failure to report and disclose a net short position, short transaction restrictions and takeover rules.

(8a) Among the data referred to in paragraph (2), the information concerning the subscriber's surname and forename, name at birth, place of residence, information on the subscriber's place of stay, the number or other identifier of the subscriber's station, the subscriber numbers calling and called by the station, the date and starting time of the call or other service and its duration may be transmitted to the Competition Authority conducting a competition supervision procedure on the grounds of the violation of the prohibition set out in section 11 or section 21 of the Act LVII of 1996 on the Prohibition of Unfair Market Practices and Restrictions of Competition, or Article 101 or 102 of the Treaty on the Functioning of the European Union, or point 26 of the Annex to the Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices

against Consumers. The unique identifier of the network and cell providing the mobile telephony service and of the equipment used in the service (IMEI), and in the case of IP networks, the identifiers used, may be provided to the Competition Authority conducting a competition supervision procedure in relation to an agreement or concerted practice between competitors to fix, directly or indirectly, purchase or sale prices, to allocate the market, including collusion in the form of competitive tendering, or to determine production or sales quotas.

(9) From among the data referred to in paragraph (2), the ones necessary for the purpose of the processing may be provided within the retention period specified in paragraph (3):

(a) to the parties carrying out billing, claims management, distribution management or customer information on behalf of the electronic communications service provider;

(b) to bodies entitled by law to settle billing and distribution disputes;

(c) to the bailiff as provided for in the Judicial Enforcement Act;

(d)

(e)

(10) The electronic communications service provider shall, upon request, provide or make available the data available to the electronic communications service provider pursuant to paragraph (2) for the purpose of ensuring the performance of the statutory duties of a court, prosecution office, investigative authority or body conducting preparatory proceedings, and national security service, which are entitled to request data pursuant to a separate Act.

(10a) For the purpose of ensuring the collection of statistical data by means of telephone contact with natural person subscribers in the course of the performance of the tasks of the Central Statistical Office (hereinafter referred to as the HCSO) as defined by an Act of Parliament, the electronic communications service provider shall, upon request, provide or make available to the HCSO the following data, in respect of the natural persons specified in the request:

(a) the number allocated to the subscriber on the basis of the subscriber identification data provided for the natural person, where the natural person has a subscription with the electronic communications service provider, or

(b) information that the natural person does not have a subscription with the electronic communications service provider.

(10b) The electronic communications service provider shall not use the personal data obtained in the course of a data request pursuant to paragraph (10a) for any other purpose and shall delete them immediately after the data have been provided.

(10c) The HCSO shall process the data received in the statistical data production process for as long as it is justified for the purpose of performing such process. The personal data and the subscriber station number shall be stored separately by the HCSO, which may link these two sets of data only for the duration of the data collection organisation and the interview. When the task is terminated, in particular after the end of each data collection, the data received in connection with it shall be deleted by the HCSO.

(11) The electronic communications service provider shall, if available to it, at the request of the offence authority, and for the purpose of identifying the offender of an offence involving the use of emergency numbers for purposes other than those for which they were intended, provide the following information in respect of the telephone number from which a call was made to the emergency number

(a) the subscriber's surname and forename, place and date of birth, mother's maiden name and forename, address and address for service of notifications; or

(b) in the case of a subscriber who is not a natural person, the business name, registered office, place of business, surname and forename of its representative."

"Section 159/A (1) For the purpose of ensuring the performance of the statutory tasks of the court, prosecution office, investigative authority or body conducting preparatory proceedings and national security service entitled to request data under a specific Act of Parliament, or in order to provide data at their request, the operator of an electronic communications network or the provider of an electronic communications service shall retain the following data generated or processed by the provider in connection with the provision of the electronic communications service concerned, relating to the use of the electronic communications service by the subscriber or user:

(a) the subscriber's personal data recorded in an individual subscriber contract in the case of fixed telephone or mobile radio telephone services, Internet access services, Internet telephony services, Internet mail services or a combination thereof;

(b) in the case of fixed or mobile telephone services, Internet access services, Internet telephony services, Internet mail services or a combination thereof, the subscriber's, user's terminal equipment or subscriber access point's caller identification number or other permanent technical identifiers necessary for the unique identification of the subscriber or user, as set out in the subscriber contract or otherwise assigned to the subscriber or user by the electronic communications service provider;

(c) in the case of fixed telephony, fixed Internet access services or a combination thereof, the address and type of installation of the subscriber, user terminal equipment or subscriber access point;

(d) in the case of fixed or mobile telephone services, Internet access services, Internet telephony services, Internet mail services, or a combination thereof, the telephone numbers, unique technical identifiers, user identifiers of the subscribers or users involved in the communication, the type of electronic communications service used, the date, starting and ending time of the communication;

(e) in the case of call forwarding and call forwarding using fixed or mobile telephony or a combination of fixed and mobile telephony, the intermediate subscriber or user numbers involved in the call set-up;

(f) in the case of mobile radio telephone services, the device identifier (IMEI) and the mobile subscriber identifier (IMSI) of the parties involved in the communication used when using the service;

(g) in the case of mobile radio telephony, the network and cellular identifier of the service provider at the time of the initiation of the communication and at the time of the provision of the service, the actual geographical location of the cell associated with that cellular identifier;

(h) in the case of Internet electronic mail, Internet telephony or a combination thereof, the data referred to in point (d) concerning the communication initiated towards the intended recipient;

(i) in the case of Internet access, Internet e-mail, Internet telephony or a combination thereof, the type of electronic communications service and the date, start and end time of the use of the service by the subscriber or user, the IP address used, the user ID, the calling number;

(j) in the case of Internet access, Internet e-mail, Internet telephony or a combination thereof, the data necessary to track any transformation of the unique technical identifiers of subscribers or users by the electronic communications service provider (IP address, port number);

(k) in the case of prepaid anonymous calling card mobile radio telephone services, the date and time of the first use of the service and the mobile phone number from which the activation was made.

(2) The data retention and reporting obligations provided for in paragraph (1) shall also apply to the data referred to in paragraph (1) generated or processed during unsuccessful calls.

(3) In order to comply with the data reporting obligation under paragraph (1), the electronic communications service provider shall retain the data specified in points (a) to (c) of paragraph (1) for one year after the termination of the subscriber contract, the data specified in points (d) to (k) for one year after they are generated, and the data specified in paragraph (2) for six months after they are generated.

(4) When providing the data referred to in paragraph (1), the body authorised to request the data shall be responsible for the lawfulness of the request. The provider of electronic communications services shall be responsible for the completeness, quality and timeliness of the data stored pursuant to paragraph (1) and of the provision of data pursuant to paragraph (1).

(5) An electronic communications service provider required to retain data pursuant to paragraph (1) may only entrust the task of data retention to another undertaking as a data processor and may only store the retained data in another Member State of the European Economic Area if the data retention contract concluded with the data processor contains security and access requirements for access to the retained data that comply with the domestic confidentiality and classified data protection rules applicable to data requests pursuant to paragraphs (1) to (2). An electronic communications service provider may not store the retained data in the territory of a country or entrust the task of data retention to a data processor in a country which is not a member of the European Economic Area.

(6) For the purposes of this section, a communication is an exchange or transmission of information between a finite number of parties by means of an electronic communications service, which includes unsuccessful calls. For the purposes of this section, a communication does not include information transmitted to the public as part of a broadcasting service over an electronic communications network unless the information can be linked to an identifiable subscriber or user who receives it.

(7) Organisations entitled to request data under a special Act of Parliament shall produce statistics annually and transmit them to the European Commission. The statistics shall include the following:

(a) the cases in which the service provider has provided data to the competent authorities pursuant to this section,

(b) the date of retention of the data under this section and the time elapsed between the date on which the competent authority requested the transmission of the data,

(c) the cases in which the provider has been unable to comply with requests for data."

[16] The constitutional complaint is unfounded.

[17] 1 The Constitutional Court found that the statutory provisions challenged in the petition transposed into Hungarian law certain mandatory rules, allowing no discretion by the Member States, of 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"). However, the Grand Chamber of the Court of Justice of the European Union (hereinafter "CJEU") ruled on the invalidity of the Directive in the Digital Rights Ireland judgement of 8 April 2014, C-293/12 and C-594/12, EU:C:2014:238 (hereinafter: "Digital Rights Ireland judgement"). According to the judgement, requiring the retention of electronic communications metadata in general terms, without differentiating the purpose and without safeguards limiting public access, constitutes a disproportionate interference with Articles 7-8 of the Charter of Fundamental Rights of the European Union (hereinafter: "EU"), which guarantee the right to privacy and the protection of personal data. As a result of this regulatory context, the Constitutional Court has paid particular attention in the present decision to the decisions of the CJEU and the constitutional courts of the EU Member States concerning the relevant EU and national legislative norms. From the case law of the CJEU, the Constitutional Court has, for the purposes of the present decision, taken into account, in addition to the Digital Rights Ireland judgement, the Privacy International judgement of 6 October 2020, C-623/17, EU:C:2020:790 (hereinafter: "Privacy International judgement").

[18] From among the decisions transposing the Directive and annulling national legislation, the Constitutional Court considered in particular the reasoning in the decision BverfG, 1 BvR 256/08 vom 2.3.2010 of the German Constitutional Court, in the joint decisions G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012 of the Austrian Constitutional Court, in the decision U-I-65/13 of the Slovenian Constitutional Court and in the decision Pl. ÚS 24/10 of the Czech Constitutional Court. In these decisions, the proceeding fora came to the overall conclusion that, in the absence of sufficient safeguards linking the retention and provision of data to law enforcement, national security and defence purposes, and containing security provisions appropriate to the nature and quantity of the data, the restriction does not meet the requirements of necessity and proportionality. The Constitutional Court stressed that these decisions do not have a binding legal force in its own decision-making, but, given the character of the case, it is nevertheless justified to take into account the constitutional theses they set out in the light of the constitutional dialogue.

[19] 2 Since the petitioner consistently invoked the violation of the fundamental rights to privacy and to the protection of personal data in a coherent manner, the

Constitutional Court conducted its examination accordingly, but in view of the fact that the data listed in section 159/A (1) of the AEC qualify as personal data (see: CCRul, Reasoning [21]).

[20] The Constitutional Court notes that the data concerned, on the one hand, concern personal data of several persons, and on the other hand, they are more than just separate, individual personal data: they are a set of data of such a mass and quality concerning the contacts and communication habits of the data subject that they may reveal a very decisive and important part of the communication profile and personality of the data subject. Moreover, since the personal data concerned are predominantly personal data specific to the contact of the data subject and because the totality of the personal data allows conclusions to be drawn about the whole set and network of contacts of the data subject, the data set concerned is more closely related to the right to privacy and, in that context, to human dignity than individual, separate personal data in general.

[21] Following the entry into force of the Fundamental Law (more specifically the entry into force of the Fourth Amendment to the Fundamental Law on 1 April 2013), the right to the protection of personal data was enshrined in the first sentence of Article VI (2) of the Fundamental Law, and since the Seventh Amendment to the Fundamental Law of 28 June 2018, the right to the protection of personal data is enshrined in the first sentence of Article VI (3), however, the Fundamental Law does not provide a constitutional definition of personal data {see Decision 2/2014. (I.21.) AB (hereinafter: CCDec 1), Reasoning [11]}. In paragraph [55] of its reasoning in Decision 11/2014 (IV.4.) (hereinafter: CCDec2), the Constitutional Court – in the context of the interpretation of Article VI of the Fundamental Law – stated that "personal data is in any case information about the private and family life of a person". Paragraph [17] of the reasoning of Decision AB 3038/2014 (III.13.) also confirms that "the Fundamental Law does not define the concept of personal data. However, it regulates the right to the protection of personal data among the rights to the protection of privacy (private and family life, private home, reputation). Although the Fundamental Law protects privacy in a broader scope than the previous Constitution (not only the private home and private secret, but also private and family life, the home and the right to communicate enjoy protection), none of the differences in itself makes it impossible to apply the principles laid down in previous decisions of the Constitutional Court appropriately."

[22] In paragraph [87] of the reasoning of Decision 32/2013 (XI.22.) AB (hereinafter: CCDec3), the Constitutional Court upheld and confirmed the interpretation of the right to informational self-determination as developed in the previous case-law of the Constitutional Court (as a general rule, everyone decides on the disclosure and use of his or her personal data, but the law may exceptionally – for a precisely defined purpose – order the disclosure of personal data, and may prescribe the manner of its use). As

pointed out by the Constitutional Court also in CCDec3, “the Fundamental Law defines relation between the individual and the community by focusing on the individual being tied to the community, without, however, affecting his or her individual value. This follows from in particular from Article O) and Article II of the Fundamental Law. Therefore, the previous case-law of the Constitutional Court interpreting the right to the protection of personal data as a right to informational self-determination can be maintained in the interpretation of the Fundamental Law. The right to informational self-determination is closely related to the right to privacy and involves the decision when and within what limits an individual discloses data that may be linked to his or her person." {see also, in the context of the interpretation of the right to the protection of personal data after the entry into force of the Fundamental Law: CCDec 1, Reasoning [18]; CCDec 2, Reasoning [55]; CCDec 3, Reasoning [86] to [87]; and Decision 17/2014. (V.30.) AB, Reasoning [31]}. Paragraph [16] of the reasoning of CCDec 1 also stated that neither the Fundamental Law nor the FOIA contain any provisions that would justify a change in the interpretation of the right to informational self-determination. The Constitutional Court, in its ruling on the present case, also interpreted the right to the protection of personal data guaranteed by Article VI (3) of the Fundamental Law in the manner developed in its consistent case-law, bearing in mind the reasoning in paragraphs [30] to [34] of the Decision 13/2013 (VI.17.) AB {C.p. Decision 3046/2016. (III.22.) AB, Reasoning [29] to [44]; Decision 3171/2017. (VII.14.) AB, Reasoning [31] to [41]; Decision 3192/2017. (VII.21.) AB, Reasoning [25] to [28]}.

[23] "The wording of Article VI of the Fundamental Law on the protection of individual privacy was changed by the Seventh Amendment to the Fundamental Law of Hungary, which entered into force on 29 June 2018. According to the original text of the Fundamental Law, »(1) Everyone shall have the right to respect for his or her private and family life, home, communications and reputation. (2) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. (3) The enforcement of the right to personal data protection and the right of access to data of public interest shall be monitored by an independent authority established by a cardinal Act.« Article 4 of the Seventh Amendment to the Fundamental Law replaced Article VI of the Fundamental Law, quoted above, with the following new provision: »(1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected. Exercising the right to freedom of expression and assembly shall not impair the private and family life and home of others. (2) The State shall provide legal protection for the tranquillity of homes. (3) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. (4) The enforcement of the right to personal data protection and the right of access to data of public interest shall be monitored by an independent authority established by a cardinal Act.« The Seventh Amendment to the Fundamental Law thus raised the protection of privacy to a new

level of regulation, replacing the previous protection of a few elements of privacy with a complex, general protection that covers the intimate sphere and the broader private sphere, the family life, home life and communications of the individual. [...] In the light of the Seventh Amendment to the Fundamental Law, the Constitutional Court last dealt with the content of the fundamental right contained in Article VI of the Fundamental Law in its Decision 3167/2019 (VII.10.) AB. The decision stated that the Fundamental Law provided for the right to the protection of personal data among the rights related to the protection of privacy" {c.p. Decision 3212/2020. (VI.19.) AB (hereinafter: CCDec 4), Reasoning [43] to [44]}.

[24] The limitation of the right to the protection of personal data as a fundamental right is subject to the general criterion laid down in Article I (3) of the Fundamental Law. Accordingly, a fundamental right may be restricted only in order to protect another fundamental right or constitutional value. Such a restriction may be carried out only to the extent that it is strictly necessary and proportionate to the aim pursued, while respecting the essential content of the fundamental right. Consequently, the Constitutional Court was required to examine whether the legislative provisions challenged in the petition constituted a restriction on the right to respect for the maintenance of communications and, if so, whether that restriction was strictly necessary and proportionate to the aim pursued, in order to safeguard another fundamental right or to protect a constitutional value, while respecting the essential content of the fundamental right.

[25] Paragraph (1) of section 159/A of the AEC lists all the data for which the Act imposes data retention obligations on the operator of an electronic communications network or the provider of an electronic communications service. According to these provisions, these data are "data relating to the use of the electronic communications service by the subscriber or user" and thus relate to the circumstances of the communication itself and not to the content of the communication.

[26] Section 159/A (1) (a) and (b) of the AEC refers, inter alia, to personal data recorded in the subscription contract, the telephone number and identifiers enabling the data subject to be specifically identified, (c) to the subscriber's address (where they have a fixed telephone/internet connection) and the type of service used (telephone or internet service) and (d) to data specific to communications between the subscriber and another person (e.g. telephone number, identifiers, times). The data to be retained under point (e) will allow the identification of where the subscriber concerned has routed and forwarded his or her calls. Point (f) requires the retention of data relating to the equipment used by the subscriber concerned and by any other person communicating with him or her. The cell identifier data referred to in point (g) identifies the actual geographical location of the subscriber concerned, i.e. in practice where he or she was physically located during the call. Point (h) refers to technical data specific

to the subscriber and the other person communicating with him or her (e.g. calling number, IDs, times) during Internet correspondence and telephone calls. Data under point (i) concerns Internet communications and their characteristics (including the specific type of service, the time of access and egress to the service, the IP address used to access the service). Point (j) requires data on IP address and port number, and point (k) requires data on when and where the data subject first used the service.

[27] The above data, listed in section 159/A (1) of the AEC as data to be retained, clearly qualify as data related to the constitutionally protected communication of the petitioner. Although they do not concern the content of his or her communications, they reveal who, by what means, from where, with whom, for how long and with what frequency they communicated by telephone or via the Internet. On this basis, the Constitutional Court held that the obligation to preserve personal data imposed by section 159/A (1) of the AEC and applied in the judgement No 8.Pf.21.057/2015/5 of the Budapest-Capital Regional Court of Appeal of 7 April 2016, restricts the petitioner's right to the protection of personal data. The Constitutional Court held in CCDec4 that "the seventh amendment to Article VI of the Fundamental Law distinguishes between private individuals by not giving increased protection to the protection of personal data, the priority protection being the right to respect for private and family life and the home, through the right to privacy, on the basis of which the family, including close relatives, in particular children, are entitled to increased protection." (CCDec4, Reasoning [46]). However, it is not only possible to draw conclusions from these data about specific contacts, but also to derive a very important aspect of the identity of the person concerned, namely his or her communication profile.

[28] The communication profile (in the light of the data relating to his or her communications) is closely linked to the privacy and human dignity of the persons concerned and, as a consequence, comes close to the inviolable core of human dignity within the scope of protection of the fundamental right to the protection of personal data (which is part of the protection of privacy). This is because "taken together, such data may allow very precise conclusions to be drawn about the private lives of the persons whose data are retained, such as their daily habits, their permanent or temporary places of residence, their daily or other movements, their activities, their social contacts and the social media they visit" (Digital Rights Ireland judgement). This communication profile is therefore considered "as special information as the content of the communications themselves" (Privacy International judgement). By its very nature, and despite the fact that the law-maker of the Fundamental Law did not grant a special constitutional position to the protection of personal data *in abstracto*, this communication profile should be given enhanced fundamental rights protection, which is materialised in the provision of adequate and strict guarantees for the processing of data as required by the AEC. On this basis, the mere stockpiling retention of the data

may constitute a restriction of the fundamental right to the protection of personal data, since it potentially entails the possibility of communication profiling and thus a serious breach of fundamental rights. In the view of the Constitutional Court, the present case involves the stockpiling collection of data. Section 159/A of the AEC sets out legitimate aims in the context of data collection, but those aims are prospective and are not always realised. The Constitutional Court identified as its reason that, in the case of the vast majority of data subjects, the collection of data has no connection whatsoever with the realisation of the purposes and will not have any such connection, since the persons concerned cannot be linked to criminal offences. According to the interpretation of the Constitutional Court, a stockpiling collection of data exists if the processing is i. not at all, or at least not sufficiently, linked to evaluable, specifically defined purposes capable of being fully achieved, ii. or, although it was previously sufficiently linked, the processing continues regardless of the fulfilment or cessation of the purpose, iii. or, despite the fact that the processing is sufficiently linked to legitimate purposes, it exceeds their scope for some reason. In the context of data processing related to section 159/A of the AEC, although purposes are indicated, the processing is not in fact linked to those specific purposes at the normative level, but is merely linked to the possible realisation of those purposes in the future. The collection of data is therefore carried out for the purpose of providing data which is not sufficiently linked to a constitutionally assessable purpose on the basis of the text of the law and which defines the scope of use too broadly. In the view of the Constitutional Court, all of this exhausts the concept of the stockpiling collection of data.

[29] 3 As the Constitutional Court established the fact of restricting the relevant fundamental right, it will continue with examining whether the restriction of the fundamental right has taken place in the interest of the enforcement of another fundamental right or to protect a constitutional value, to the extent that is absolutely necessary, proportionately to the objective pursued, and respecting the essential content of such fundamental right.

[30] In addition to the mandatory legislative task arising from the implementation of the Directive, the creation of harmonisation of Hungarian and EU legislation, the contested legislative provisions were necessary in the interests of Hungary's law enforcement, national security and national defence. The Constitutional Court finds that, in the constitutional context of the present case, those interests must be regarded as having constitutional value that necessitate the restriction of the fundamental rights concerned {see the Decision 3255/2012 (IX.28.) AB, Reasoning [14]}, and that the method of restriction, namely the retention of data for a period of one or six months, is suitable for achieving the objectives pursued by the law-maker.

[31] The Constitutional Court went on to consider whether the contested legislative provisions restrict the fundamental right concerned to the extent strictly necessary.

Section 159/A (1) of the AEC provides that the operator of an electronic communications network or the provider of an electronic communications service shall retain all data relating to the use of the electronic communications service by the subscriber or user which are generated or processed by the provider in connection with the provision of the electronic communications service concerned. This essentially means that the retention obligation covers all ordinary acts involving electronic communications that are nowadays indispensable for participation in community life, without the existence of any imputable act or at least the potential of such imputable act regarding the subscriber or user concerned. The Constitutional Court finds, however, that the retention of the data concerned in the present case does not in itself restrict the right to the protection of personal data beyond what is strictly necessary. One of the reasons for that is that the data are not stored directly by the State but by other operators or service providers operating in the economic sphere, who cannot use the data covered by section 159/A (1) of the AEC for their own purposes under the contested provisions of the legislation, since the data to be retained must be kept physically and administratively separate from other data processed by the service provider. Thus, the data to be collected under the contested provision of the AEC are not in their entirety at the disposal of the data controller, the data subject or the State.

[32] On the other hand, the retention period of one or six months laid down in the contested provisions ensures that the otherwise unconditional stockpiling retention of data remains within the strictly necessary limits. The Constitutional Court stresses that the data processed for law enforcement, national security and defence purposes, as provided for by the contested provision of the AEC, are a valuable tool for the effective achievement of the objectives pursued, especially in relation to organised crime. Without knowledge of such data, law enforcement mechanisms may be hampered and the effectiveness of the criminal justice system may be reduced, since they may provide evidence that is often indispensable in the course of proceedings and cannot be replaced by other sources. Consequently, the retention and the provision of data does not always lead to an *ab ovo* violation of the Fundamental Law. At the same time, such prior, stockpiling data processing requires higher constitutional standards of proportionality, also in view of the nature and quantity of the data processed.

[33] 4 The Constitutional Court next examined whether the restriction on the right to the protection of personal data was proportionate to the aim pursued and respected the essential content of the fundamental right. The Constitutional Court examined the restriction of the fundamental right first in the context of the collection of data by the Service Provider and then in the context of access to the data. In this context, it found that the prior, stockpiling retention of data provided for in section 159/A (1) of the AEC disproportionately restricts the fundamental right concerned in relation to the aim pursued.

[34] 4.1 At the outset of applying the proportionality test, the Constitutional Court noted that in the present case the data are mostly linked to persons and that the general and preventive retention of data also affects the rights of persons who cannot be indirectly linked to the objectives pursued. Indeed, a single service provider may store and manage millions of data of millions of subscribers. Section 159/A (1) of the AEC therefore also applies to persons who are not even remotely connected with serious criminal offences, simply because they use electronic communications services. In their case, however, the constitutional values of law enforcement, national security and defence as the relevant fundamental rights justifying the restriction of fundamental rights do not in fact arise in connection with the processing of the data. In this regard, the Constitutional Court reinforces that "being bound to the purpose to be achieved is a condition of and, at the same time, the most important guarantee for exercising the right to informational self-determination. It means that personal data may only be processed for a clearly defined and lawful purpose. [...] It follows from the principle of adherence to the goal/purpose to be achieved that collecting and storing data without a specific goal, »for stockpiling«, for an unspecified future use are unconstitutional" [Decision 15/1991 (IV.13.) AB, ABH 1991, 40, 42]. However, it also follows from this, that the retention of data for stockpiling purposes does not in itself result in an *ab ovo* violation of the Fundamental Law, provided that it has a constitutionally justifiable purpose, the processing of the data is linked to that purpose and is proportionate to that purpose, within the limits of appropriate safeguards. However, in applying the proportionality test, the regulation is therefore expected to meet higher constitutional standards.

[35] 4.2 In the context of proportionality, the Constitutional Court examined first of all the issue of providing adequate information, both in relation to data retention and data provision, in view of its prominent role. This is a guarantee of the adequate protection of the rights of data subjects, without which "users of electronic communications may, in principle, rightfully expect that their communications and the data relating to them will remain anonymous and cannot be recorded in the absence of their consent" (Privacy International judgement). This information must cover both the retention and the provision of data, and data subjects must be aware of who is processing their data, for what purposes, for what reasons and to what extent. Section 159 of the AEC fulfils the requirement of prior information, also with regard to section 159/A, as it imposes an obligation on the service provider to inform the subscriber at the time of executing the subscription contract.

[36] 4.3 In the context of the proportionality of data retention, the Constitutional Court examined whether the law-maker had sufficiently ensured the security of the data to be retained, taking into account that the retained data are, given their comprehensive (communication profiling) nature, at increased risk of unlawful acquisition. The range

and volume of data processed justify that a particularly high level of protection and security should be ensured by means of the required technical and organisational measures, protecting data against accidental or unlawful destruction, as well as against accidental loss or alteration. The Constitutional Court has already established that the data subject is entitled to a guarantee that his or her data will be treated in accordance with the rules on data security [see the Decision 144/2008 (XI.26.) AB, ABH 2008, 1107, 1157], and considers that there is no obstacle to the application in the present case of the principle set out in that earlier decision {c.p. Decision 13/2013. (VI.17.) AB, Reasoning [30] to [32]}. As the data listed in section 159/A of the AEC provide for the possibility to establish a communication profile of the persons concerned, the data listed therein must be kept with particular care. Section 159/A of the AEC does not contain any data security provisions which would guarantee the protection of the retained data against the risk of misuse or any unlawful access or use. However, certain provisions of the AEC, in particular sections 155 and 156, contain data security rules applicable to all data processing by electronic communications service providers, including section 159/A. The AEC also contains rules which are adapted to the volume of data to be retained, the sensitive nature of such data and the risk of unlawful access to such data, and which are progressively extended in line with the time at which the petition was filed, and which are intended in particular to regulate clearly and strictly the protection and security of the data in question in order to ensure their full integrity and confidentiality. In fact, sufficiently strict and clear rules are needed as regards data security, data use, transparency and legal protection. The Constitutional Court refers to the data security standards formulated by the CJEU in the Digital Rights Ireland judgement, and the Constitutional Court considers the provisions of the AEC to be in line with such standards.

[37] 4.4 In its examination of the proportionality of data retention, the Constitutional Court reviewed the constitutionality of the rules on the period of data retention set by section 159/A (3) of the AEC. In this context, it found that the retention of data for one year – in the case of section 159/A (1) (a) to (c) of the AEC from the termination of the subscriber contract and in the case of section 159/A (1) (d) to (k) from the date of the creation of the data – and for six months – in the case of section 159/A (2) – can be considered proportionate to the objectives pursued. The Constitutional Court emphasises that, although the retention of the data recorded under points (a) to (c) is for an unforeseeable – but limited – period at the time of the conclusion of the contract, they are data without which the entire collection of data would be meaningless and would be rendered ineffective for the purposes pursued. The prescribed period of data retention does not, therefore, in itself give rise to a disproportionate restriction of fundamental rights, and can be considered justified and constitutionally sound if other safeguards are in place.

[38] 4.5 Following the data retention, the Constitutional Court examined the proportionality of the provision of data. The phrase "for the purpose of ensuring the performance of the statutory tasks" in section 159/A (1) of the AEC is too general and does not take into account that the constitutional proportionality of this data provision is based solely on the performance of tasks related to the law enforcement, national security and defence interests of Hungary. The court, the public prosecutor's office, the investigating authority or the body conducting the preparatory proceedings and the national security service – as those entitled to receive the data – may request the provision of the data only on the basis of a specific statutory authorisation and for the purpose of ensuring the performance of their duties, on the basis of a request. However, there is no guarantee in the AEC that the request may only be made for the purpose of ensuring the performance of their statutory tasks where the law defines the purpose as the performance of a specific law enforcement, national security or defence task. When assessing the proportionality of the provision of data, it must be borne in mind that the statutory tasks of the bodies receiving the data are much broader than the purposes which provide the constitutional framework for the provision of data. Therefore, the enforcement of these protected constitutional values should be facilitated by section 159/A (1) to the extent of limiting the obligation to retain and provide data by means of clear and precise wording to cases where the tasks of the bodies listed in the challenged provision of law under the specialised legislation are specific law enforcement, national security or defence tasks. Furthermore, the fact that section 159/A (1) of the AEC – although it is included under the subheading of Data retention for law enforcement, national security and defence purposes – does not in fact lay down any distinction, restriction or exception in relation to the procedures or the scope of serious offences in respect of which the provision of data is justified, results in a disproportionate restriction of fundamental rights in relation to the provision of data.

[39] The Constitutional Court emphasises that a restriction of a fundamental right of this nature and scope can only be imposed in a narrow niche, within a specifically limited framework and under well-defined substantive and procedural conditions. Each of these must be adapted to and linked to the constitutional values as objectives protected by the legislation. Accordingly, the constitutional basis for the provision of data should also be a criminal prosecution for specifically defined serious offences. Compliance with the proportionality criterion therefore becomes questionable not only if there are no circumstances giving rise to criminal proceedings at all, but also if there are only suspicions of minor offences. Even then, the protection of constitutional values, which *in concreto* are of lesser importance, cannot justify the restriction of the rights of millions of people. The Constitutional Court emphasises that although the detailed rules in this area are a matter for sectoral legislation, the inclusion of minimum standards in the AEC is a constitutional requirement. The reason for this is that the basis

for data processing is provided by the AEC, therefore its provisions may be expected to lay down certain – minimum – limits in addition to the basis, without which the AEC would not in fact impose any constitutional requirement of purpose limitation on data processing for the protection of personal data. As a constitutional minimum that must in any case be reflected in the ECHR, data processing may only take place in connection with the tasks of the authorised bodies in relation to specific, legitimate purposes and serious criminal offences. However, it is sufficient to regulate the details of this requirement in sectoral laws.

[40] The Constitutional Court therefore found that the contested statutory provision indeed defines too broadly the procedure, the purpose and the scope of the data that can be requested by those entitled to request data under a specific Act of the Parliament. The authorisation to transfer data is therefore too general, abstract and lacks the specificity to link and adapt the processing to its purpose. The term "in proportion to the aim pursued" included in the general criterion of the restriction of fundamental rights imposes, in the field of data processing, a particular obligation of purpose limitation (see CCDec3, Reasoning [91]).

[41] 4.6 In the context of the provision of data, the Constitutional Court also refers to the obligation arising from the decisions of the CJEU that, where authorised by law, a court or an independent administrative body not involved in the judicial process should participate in the procedure as the rightful applicant or as the preliminary reviewer of the merits of the request for data. The Constitutional Court stresses, also in the context of this criterion, that it is sufficient to lay down the detailed rules for effective review in sectoral laws, but that the requirement of review and the role of the judicial or independent administrative body not involved in the criminal proceedings must also be reflected in the AEC, which lays down the basis for data processing. The Constitutional Court concludes that the AEC does not comply in this respect with the regulatory requirements arising from the Fundamental Law and the decisions of the CJEU.

[42] 4.7 On the basis of the above, the Constitutional Court finds that section 159/A (1) of the AEC disproportionately infringes the petitioner's right to privacy under Article VI (1) of the Fundamental Law and the right to protection of personal data under Article VI (3) of the Fundamental Law, i.e. it is contrary to the Fundamental Law. However, the Constitutional Court held that the incompatibility between the legislation and the right to privacy and the right to the protection of personal data could be remedied without annulling the contested legislation, by applying other legal remedies available to the Constitutional Court. Indeed, the injury of the relevant fundamental rights does not stem from the legislation but from its incompleteness.

[43] Section 46 (1) of the ACC empowers the Constitutional Court to call upon the body that committed an omission to fulfil its duty, together with specifying the time limit, if, in the course of its proceedings in the exercise of its powers, it finds an infringement of the Fundamental Law caused by the law-maker's omission. According to paragraph (2) c) of the relevant statutory regulation, the omission of the law-maker's tasks may be established when the essential content of the legal regulation that can be derived from the Fundamental Law is incomplete.

[44] According to the Constitutional Court, in the case of the statutory provision examined in the present proceedings, it is possible to act in accordance with the powers granted to it under section 46 of the ACC, in a manner that saves the law in force. The Constitutional Court found that the violation of the Fundamental Law by the regulation was due to the fact that the law-maker failed to create an adequate regulatory environment for data processing for law enforcement, national security and defence purposes, and regulated the given issue too broadly, without sufficient limits and conditions.

[45] For this reason the Constitutional Court held that the restitution of compliance with the Fundamental Law requires the supplementing of the text in force rather than the annulment of the contested provision. This will ensure that the legislation protecting key constitutional values is in line with the Fundamental Law.

[46] Therefore, the Constitutional Court, acting *ex officio*, found, on the basis of section 46 (2) (c) of the ACC, that the Parliament had caused an infringement of the Fundamental Law by failing to regulate in section 159/A of the AEC the processing of personal data for law enforcement, national security and defence purposes in line with the consequences of the right to respect for privacy under paragraph (1) and the right to the protection of personal data under paragraph (3) of Article VI of the Fundamental Law. The Constitutional Court therefore called upon Parliament to meet its legislative duty by 31 December 2022.

[47] 5 The Constitutional Court, exercising the right granted by Article 24 (4) of the Fundamental Law, notes the following. Although the Constitutional Court has stated above that the data collected pursuant to section 159/A (1) of the AEC are not available, on the basis of this provision of the law, in their entirety to the data controller, the data subject or the State, this finding is overruled by section 157 (2) of the AEC. That provision provides for the mandatory retention, for a dual purpose, of data which are almost identical to those concerned by the provision at issue in the complaint. Accordingly, the data to be stored include, among others, the calling and called subscriber numbers, the starting time and duration of the call, the cellular information and, in the case of IP networks, the identifiers used. The purpose of data retention under paragraph (2a) is the billing of the subscriber and the collection of related

charges, as well as the monitoring of subscriber contracts. Paragraph (3) specifies as a different purpose the fulfilment of data requests by specified bodies in connection with the performance of their statutory tasks. Under paragraph (10), "the electronic communications service provider shall, upon request, provide or make available" the data collected this way "for the purpose of ensuring the performance of the statutory duties of a court, prosecution office, investigative authority or body conducting preparatory proceedings, and national security service, which are entitled to request data pursuant to a separate Act". In practice, therefore, the collection of data pursuant to section 157 (2) and section 159/A (1) of the AEC leads to the same result, irrespective of the different purpose, following a request for data: the authorities have access to the data thus retained. In this sense, there is a close substantive link between the relevant provisions of the law.

[48] The Constitutional Court has held that the arguments set out above in relation to section 159/A of the AEC, in the case of which such an interpretation is possible, must also apply to the obligation to retain and supply data imposed by section 157 for the purpose of enabling the public authorities to carry out their tasks. Only a summary of these is given below. Despite the fact that section 157 (2) of the AEC provides for data retention in a narrower scope than section 159/A (1), the Constitutional Court found that the identity and movement profile of the data subjects can also be created from this more limited range of data, thus a restriction of the protection of personal data is realized. Furthermore, the Constitutional Court found from a combined interpretation of section 157 (2) and (3) of the AEC that, in the context of paragraph (3), purpose limitation is not enforced, since the stockpiling collection of data is linked to an unforeseeable future purpose. In itself, the "the fulfilment of data requests by specified bodies in connection with the performance of their statutory tasks" – which is in fact realised in the obligation to hand over and make available the data referred to in paragraph (10) – does not give rise to a situation of competing fundamental rights which would meet the criteria for the restriction of fundamental rights under Article I (3) of the Fundamental Law. In the light of the foregoing, the Constitutional Court finds that the provisions under section 157 of the AEC also fail to fully comply with the requirements of Article VI (1) and (3) of the Fundamental Law, and the findings of the Constitutional Court set out above in relation to the infringement of the Fundamental Law manifested in an omission apply to that section, too.

[49] 6 The Constitutional Court notes that the fact of prior processing for a purpose laid down in an Act of Parliament does not necessarily in itself constitute a disproportionate infringement of the fundamental right to the protection of personal data. It is the law-maker's duty to make the collection and supply of data compatible with the constitutional criteria for the restriction of fundamental rights by incorporating into the legislation appropriate safeguards which are currently lacking. As a

consequence, by providing for a stricter than general statutory guarantee of the constitutionally protected principles of data processing (data security, purpose limitation, restricted use, transparency, legal remedies, etc.), also this type of data processing could be carried out constitutionally.

IV

[50] Based on the second sentence of section 44 (1) of the ACC, the Constitutional Court orders the publication of the decision in the Hungarian Official Gazette.

Budapest, 28 June 2022.

Dr. Tamás Sulyok,
President of the Constitutional Court
rapporteur, Justice of the Constitutional Court

Dr. Ágnes Czine, Justice of the Constitutional Court

Dr. Egon Dienes-Oehm, Justice of the Constitutional Court

Dr. Tünde Handó, Justice of the Constitutional Court

Dr. Attila Horváth, Justice of the Constitutional Court

Dr. Ildikó Hörcherné dr. Marosi, Justice of the Constitutional Court

Dr. Tamás Sulyok, President of the Constitutional Court on behalf of Justice *dr. Imre Juhász* unable to sign

Dr. Miklós Juhász, Justice of the Constitutional Court

Dr. Zoltán Márki, Justice of the Constitutional Court

Dr. Tamás Sulyok, President of the Constitutional Court on behalf of Justice *dr. Béla Pokol* unable to sign

Dr. László Salamon, Justice of the Constitutional Court

Dr. Balázs Schanda, Justice of the Constitutional Court

Dr. Marcel Szabó, Justice of the Constitutional Court

Dr. Tamás Sulyok, President of the Constitutional Court on behalf of Justice *dr. Péter Szalay* unable to sign

Dr. Mária Szívós, Justice of the Constitutional Court