Decision 3110/2022 (III. 23.) AB

on the annulment of a judicial decision

The plenary session of the Constitutional Court, in the subject-matter of a constitutional complaint – with concurring reasonings by Justices *dr. Ildikó Hörcherné dr. Marosi* and *dr. Balázs Schanda* – adopted the following

decision:

The Constitutional Court establishes that the judgement No. Kfv.II.37.001/2021/6 of the Curia and the judgement No. 105.K.706.125/2020/12 of the Budapest-Capital Regional Court are contrary to the Fundamental Law and, therefore, annuls them.

Reasoning

I

[1] 1. The National Authority for Data Protection and Freedom of Information, as the petitioner (hereinafter: petitioner or Authority), through its legal representative (Dr. Gábor Dudás, attorney-at-law), submitted a constitutional complaint pursuant to section 27 (1) of the Act CLI of 2011 on the Constitutional Court (hereinafter: ACC).

[2] 1.1. On the basis of a notification, the petitioner initiated a data protection investigation procedure and subsequently an ex officio data protection authority procedure against the controller in relation to the processing of data concerning the collection of signatures to force joining the European Public Prosecutor's Office. In its decision, it found that the controller collected personal data of the data subjects for contact purposes without a legal basis between 19 July 2018 and 30 May 2019, and did not provide adequate information on all relevant circumstances of the processing, thereby violating several provisions of the Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (hereinafter: GDPR). In the reasoning of its decision, it also found that the processing infringed the fundamental principle of fair processing under the GDPR by failing to provide data subjects with adequate information about the purposes of the processing. The petitioner ordered the controller to erase the

personal data collected without legal basis for the purpose of the contact and ordered it to pay a data protection fine of HUF 1 000 000.

[3] 1.2. The Budapest-Capital Regional Court, acting on the controller's claim for action, annulled the provisions of the petitioner's decision concerning the erasure of personal data collected without legal basis, the provision of proof of compliance with this obligation and the enforcement in case of non-compliance. As the basis of the judgement, the court indicated that, in the specific case, the petitioner could only apply the legal consequences set out in the GDPR against the controller in accordance with the Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Freedom of Information Act). In interpreting the relevant provisions of the GDPR in the case under review, the Budapest-Capital Regional Court concluded that data can only be erased at the request of the data subject, the petitioner is not entitled to order such deletion ex officio, and its provision to this effect is null and void for the breach of its powers.

[4] 1.3. Both parties lodged an application for review of the first instance judgement with the Curia, which rejected the controller's application on procedural grounds and upheld the first instance judgement despite the petitioner's request. The Curia held that the contested part of the petitioner's decision was not suitable for review because the petitioner had failed to comply with its obligation to state reasons. It also held that neither the application for review nor the counter-application disputed that the court of first instance had examined the legal basis of a decision that was inadequately reasoned, partly of its own motion and partly on the basis of new arguments put forward by the respondent, and that the Curia had therefore examined the merits of the case in relation to the statements made in the judgement concerning further references about the legal basis. In this context, the Curia – based on the combined interpretation of Article 58 (2) (g) of the GDPR on data erasure and Article 17 on the right to data erasure –fully agreed with the legal position of the Regional Court on the interpretation of the GDPR that data erasure can only take place upon the request of the data subject, thus the Regional Court's finding that the petitioner lacked the power to order the erasure ex officio was justified.

[5] 2. The petitioner then lodged a constitutional complaint with the Constitutional Court because, in its view, the judgement No. 105.K.706.125/2020/12 of the Budapest-Capital Regional Court and the judgement No. Kfv.II.37.001/2021/6 of the Curia violate Articles B (1), E (2) and (3), Article I (3), Article VI (3) and (4) and Article XXVIII (1) and (7) of the Fundamental Law. In its view, the contested judicial decisions restrict the powers granted to it by the Fundamental Law in a manner contrary to the Fundamental Law and result in a serious disruption of its functioning, and are therefore in conflict with the Fundamental Law. In view of all this, it requested the Constitutional Court to declare that the challenged judicial decisions are contrary to the Fundamental Law and

to annul them. It also submitted a request for a stay of execution of the judgements concerned.

[6] 2.1. The petitioner put forward the following pleas in relation to the limitation of its powers contrary to the Fundamental Law and the disruption of its functioning, arising from a breach of Article B (1), Article E (2) to (3) and Article VI (3) to (4) of the Fundamental Law. It stressed that, among other things, it has long had the power to order ex officio the erasure of data processed unlawfully. He explained the need for the creation of the GDPR due to external circumstances – technological development, globalisation, the increasing value of data, the explosion in the number of data subjects – and the purpose of the norm itself: to strengthen the level of data protection protection and, with it, the powers of supervisory authorities. Consequently, according to the petitioner, it is an emptying of the power of control granted by the Fundamental Law if it can only carry out formal control without any real means of intervention. If a claim can only be enforced under the procedure adopted by the challenged judicial decisions, the data subject must first request the controller to erase his or her personal data, and then may the petitioner proceed under Article 77 of the GDPR. In the case of unlawful data processing involving hundreds of thousands or millions of data subjects, this can mean an unmanageable amount of administrative cases for the petitioner's operation, and it also has a negative impact on the enforcement of the data subject's rights, where the personal data remain in the – unlawful – management of the controller without any meaningful supervisory control until the case is closed. According to the petitioner, although Article VI (4) of the Fundamental Law does not define the content of the control, it is not an empty provision since its normative content is provided by Article VI (3) to (4) in combination with Article E (2) to (3). The exclusion of the petitioner from the ex officio erasure of unlawfully processed data is contrary to this power established with normative content, as it deprives the data protection authority of the possibility to remedy the breach in a substantive, effective and efficient way, and consequently reduces the level of fundamental rights protection previously achieved, and in practice leads to serious dysfunctions.

[7] The petitioner also interpreted that the courts reached the contested findings by a mere grammatical interpretation of the GDPR, which is contrary to Article 28 of the Fundamental Law, especially considering that, according to the petitioner, an interpretation in conformity with the Fundamental Law can also be reached by an adequate – and still grammatical – interpretation of the provisions of the law, in a way different from the direction followed by the courts. In the petitioner's view, the fact that the courts in charge of the proceedings reached a result that was clearly contrary to the Fundamental Law in the interpretation of legal norms, and did not actually interpret the legislation but overwrote it, constituted a legislative act *contra legem*, or even *contra consitutionem*, in a manner violating legal certainty. This, in the petitioner's view,

also raises a violation of the right to a fair trial in the present case, since the court has thereby freed itself from the principle of being bound by the law. Furthermore, the petitioner referred to the fact that the contested interpretation of the law was also contrary to the requirement of legal certainty at EU level, as it is contrary to the requirement of consistent and uniform implementation – textually laid down, among others, in the GDPR [recital 129 of the GDPR] – given that, according to the petitioner, the right to order ex officio data erasure is also recognised by other supervisory authorities.

[8] 2.2. In relation to the infringement of Article XXVIII (1) and (7) of the Fundamental Law, the petitioner submitted that both the Regional Court and the Curia failed to initiate the preliminary ruling procedure – which, according to the petitioner, was mandatory under the CILFIT case 283/81 of 6 October 1982, EU:C:1982:335 (hereinafter "CILFIT") – in relation to the relevant provisions of the GDPR. This violated the petitioner's right to a fair trial and remedy, and limited its power of control, in particular as all aspects of EU law remained unexplored and the relevant provisions were interpreted by distancing it from the purpose of the legal norm. This violation of fundamental rights has therefore occurred in the absence of sufficient reflection in the context of EU law. The violation of the fundamental rights referred also resulted from the fact that, in the petitioner's view, the courts in charge did not fulfil their obligation to state reasons, did not examine its observations on the merits of the case in sufficient depth, and, in breach of the obligation to be bound by the application for review, the Curia examined issues that were not the subject of the review proceedings.

[9] 2.3. The petitioner also requested that the Constitutional Court suspend the enforcement of the judgements complained of. The underlying reason for this is that the petitioner is still conducting a number of data protection authority proceedings at the time of adopting the decision and these proceedings are materially affected by the contested decisions, as due to these decisions the petitioner cannot validly and effectively order any data erasure measure. According to the petitioner, this would also prevent the GDPR from being undermined in its uniform application in the EU.

[10] 2.4. In the course of its proceedings, the Constitutional Court requested the Minister of Justice to express her professional opinion.

[11] In her response to the request, the Minister of Justice – in addition to providing a detailed overview of the domestic and international regulatory environment and the decisions of the Constitutional Court under the old Constitution – emphasised, on the basis of the principle of the division of powers laid down in Article C (1) of the Fundamental Law, that the constitutional complaint concerns the content of the challenged judicial decisions and not the applicable law, and therefore it cannot assess the content of the judgements. She stressed that the Court of Justice of the European

Union is empowered to provide a final, authoritative interpretation of the GDPR. She pointed out that the most significant achievements of the right to informational self-determination are principles – requiring continuous enforcement – that can also be derived from Article VI (3) of the Fundamental Law. Control by the data protection supervisory authority (the possibility to intervene) is and should be ensured under both the Fundamental Law, EU law and international law obligations, and was widely and uncontroversially ensured in the pre-GDPR regime. According to Article 57 (1) (a) of the GDPR, the provisions of the GDPR are to be enforced by data protection supervisory authorities, and this enforcement should not be limited to data subjects who have detected a breach and lodged a complaint, as these provisions affect all data subjects. The so-called "remedial powers" granted under the GDPR also include the possibility for data protection supervisory authorities to require controllers to bring their processing into compliance with the GDPR (which may include the erasure of unlawfully processed personal data), and the Government is not aware of any contrary interpretation of the law in the context of the implementation of the GDPR in the Member States. A divergent interpretation of the law would lead to a seriously disadvantageous, constitutionally unjustifiable situation for data subjects, as a situation would arise in which many data subjects would not have access to legal protection in the application of the GDPR in the absence of an explicit expression of their will, and in such a case data subjects of data processing under the Freedom of Information Act would have access to such protection, thus creating unconstitutionally unjustified different (discriminatory) and divergent regimes. She stressed that with the amendment of the Freedom of Information Act, which will enter into force on 1 January 2022, the legislator sought to clarify and specify the interpretation in order to facilitate a uniform interpretation of the law, granting precedence to EU law.

II

[12] 1. The provisions of the Fundamental Law affected by the petition:

"Article E (2) In order to participate in the European Union as a Member State, and on the basis of an international treaty, Hungary may, to the extent necessary to exercise the rights and fulfil the obligations set out in the founding treaties, exercise some of its competences deriving from the Fundamental Law jointly with other Member States, through the institutions of the European Union. Exercise of competences under this paragraph shall comply with the fundamental rights and freedoms provided for in the Fundamental Law and shall not limit the inalienable right of Hungary to determine its territorial unity, population, form of government and state structure.

The law of the European Union may, within the framework set out in paragraph (2), lay down generally binding rules of conduct."

"Article VI (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."

"Article 28 In the course of the application of law, courts shall interpret the text of laws primarily in accordance with their purpose and with the Fundamental Law. In the course of ascertaining the purpose of a law, consideration shall be given primarily to the preamble of that law and the justification of the proposal for or for amending the law. In the interpretation of the Fundamental Law and of the laws one should assume that they serve a moral and economic purpose, which is in line with common sense and the public good."

[13] 2. The relevant provisions of the GDPR:

"Article 17 Right to erasure ("right to be forgotten")

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) | the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6 (1), or point (a) of Article 9 (2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21 (1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8 (1).

(2) Where the controller has made the personal data public and is obliged pursuant to paragraph (1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs (1) and (2) shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9 (2) as well as Article 9 (3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims."

"Article 58

Powers

(1) Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42 (7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

(2) Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17 (2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

(4) The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

(5) Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial

authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

(6) Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs (1), (2) and (3). The exercise of those powers shall not impair the effective operation of Chapter VII."

[14] 3. Pursuant to the Act CXXII of 2021 amending certain Acts on justice and related matters (hereinafter referred to as the "Amendment Act"):

"Section 65 Section 61 (1) a) of the Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information shall be replaced by the following provision:

[In its decision adopted in the data protection authority procedure, the Authority]

»(a) in relation to the data processing operations specified in section 2 (2) and (4), apply the legal consequences specified in the General Data Protection Regulation, in particular, upon request or ex officio, order the erasure of personal data processed unlawfully in a manner specified by the Authority, or otherwise restrict processing temporarily or permanently;«

[15] 4. The relevant provisions of the Freedom of Information Act:

"Section 2 (1) The scope of this Act shall, with regard to personal data, as defined in paragraphs (2) to (6), cover all data processing that relates personal data and data of public interest or data public on grounds of public interest.

(2) The General Data Protection Regulation shall apply to the processing of personal data covered by Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as the General Data Protection Regulation), with the amendments specified in Chapters III to V and in Chapter VI/A as well as section 3 points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24, section 4 (5), section 5 (3) to (5), (7) and (8), section 13 (2), section 23, section 25, section 25/G (3), (4) and (6), section 25/H (2), section 25/M (2), section 25/N, section 51/A (1), sections 52 to 54, section 55 (1) to (2), sections 56 to 60, section 60/A (1) to (3) and (6), section 61 (1) a) and c), section 61 (2) and (3), (4) b) and (6) to (10), and sections 61/A to 61/D, sections 62 to 71, section 72, section 75 (1) to (5), section 75/A and Annex 1.

(3) This Act applies to the processing of personal data for law enforcement, national security and defence purposes.

(4) The provisions set out below shall apply to the processing of personal data not covered by paragraphs (2) and (3):

(a) Article 4, Chapters II to VI and VIII to IX of the General Data Protection Regulation; and

(b) Chapters III to V and in Chapter VI/A as well as section 3 points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24, section 4 (5), section 5 (3) to (5), (7) and (8), section 13 (2), section 23, section 25, section 25/G (3), (4) and (6), section 25/H (2), section 25/M (2), section 25/N, section 51/A (1), sections 52 to 54, section 55 (1) to (2), sections 56 to 60, section 60/A (1) to (3) and (6), section 61 (1) a) and c), section 61 (2) and (3), (4) b) and (6) to (10), and sections 61/A to 61/D, sections 62 to 71, section 72, section 75 (1) to (5), section 75/A and Annex 1 of this Act."

III

[16] 1. The Constitutional Court first examined whether the constitutional complaint complied with the formal and substantive statutory conditions for the admissibility of a constitutional complaint.

[17] The provisions of section 27 of the ACC in force at the time of the examination of the motion: "(1) According to Section 24 (2) (d) of the Fundamental Law, persons or organisations affected in an individual case may submit a constitutional complaint to the Constitutional Court against a judicial decision contrary to the Fundamental Law, if the decision adopted in the merits of the case or another decision terminating the judicial proceedings (a) violates the petitioner's right granted in the Fundamental Law or restricts its powers in breach of the Fundamental Law, and (b) the possibilities for legal remedy have already been exhausted by the petitioner or no possibility for legal remedy is available for him or her.

(2) Regardless of their legal status, persons or entities shall be deemed to be affected if (a) they were parties to the court proceedings, (b) the decision contains a provision concerning them, or (c) the decision of the court concerns their right, obligation or the lawfulness of their conduct.

(3) In the case of a petitioner exercising public authority, it shall be examined whether the right guaranteed by the Fundamental Law, as indicated in the petition, is vested in the petitioner."

[18] In the context of the examination of the petitioner's entitlement [section 51 (1) of the ACC], the Constitutional Court points out that pursuant to section 27 (1) of the ACC, an organisation exercising public authority [in this case, an independent authority under Article VI (4) of the Fundamental Law] is also entitled to lodge a complaint under section 27 of the ACC. {Cf. Decision 33/2021. (XII. 22.) AB, Reasoning [14]}.

[19] In accordance with section 30 (1) of the ACC, the constitutional complaint under section 27 of the ACC may be submitted within sixty days from the date of delivery of the challenged decision. The decision of the Curia on which the constitutional complaint is based was received by the legal representative of the petitioner on 7 May 2021, and the constitutional complaint was filed on 26 May 2021, within the deadline. The applicant's legal representative has attached his power of attorney. The petition complies with the criteria for an explicit request laid down in section 52 (1b) (a) to (f) of the ACC. The petitioner is not only entitled to take action, but also affected in the case under examination, because it was a party to the court proceedings [section 27 (2) (a) of the ACC].

[20] 2. According to section 55 (4a) of the ACC: "The merits of a petition challenging a limitation of the powers of a petitioner exercising public authority shall be considered only if the decision challenged (a) results in a serious disruption of the petitioner's operations, or (b) infringes any of its powers provided for in the Fundamental Law."

[21] The petitioner based its constitutional complaint on both subsections of section 27 (1) (a) of the ACC, i.e. it claimed both a violation of the rights guaranteed by the Fundamental Law and a restriction of its powers in violation of the Fundamental Law. Since these are alternative conditions that justify a different examination, the Constitutional Court assessed the petition according to its content as a complaint related to powers under the second subsection of paragraph (1) of section 27 of the ACC. In view of the fact that the petitioner has expressly invoked a limitation of its powers, it must therefore prove that these powers are expressly granted by the Fundamental Law or that the infringement of its powers causes a serious disruption of its functioning [section 55 (4a)].

[22] In examining these conditions, the Constitutional Court emphasises the following. The Constitutional Court points out that in Hungary, on the basis of a cardinal Act adopted on the basis of the authorisation of the Fundamental Law, the petitioner is an Authority, which is independent of the Government in the field of data protection and freedom of information, recognised by the institutions and law of the European Union, and its head is elected by the Parliament. Thus, in the present case, the petitioner is an independent authority established by a cardinal Act on the basis of Article VI (4) of the Fundamental Law, whose constitutional task is to monitor the enforcement of the right to the protection of personal data and the right to access data of public interest under the Fundamental Law. As a result of the legal status of the petitioner, which is established in the Fundamental Law as described above, the petitioner's powers and duties are established in the Fundamental Law, with the detailed rules being contained in the Freedom of Information Act – which is a cardinal Act under the Fundamental Law – and the GDPR. In the case under examination, the task assigned by the Fundamental Law cannot be separated from the powers deriving from the Fundamental Law, since

the petitioner can perform its constitutional task through the powers laid down in the cardinal Act. Therefore, the condition set under section 55 (4a) (b) of the ACC is complied with. The Constitutional Court found that the condition under paragraph (4a) (a) is also fulfilled, as the interpretation of law contained in the challenged judicial decisions in the case under review, based on the petition, is capable of hindering the effective performance of the petitioner's task assigned by the Fundamental Law, and therefore of causing serious disruption to the petitioner's operation (significantly impeding its ability to intervene in order to protect the fundamental right guaranteed by the Fundamental Law). The petitioner's activity is hampered if it cannot order ex officio the erasure of a large number of unlawfully processed data when it initiates proceedings in order to protect the rights of a large number of data subjects (the multitude of data subjects). On the basis of the above, there is no obstacle to adopting a decision on the merits of the petition.

[23] According to section 29 of the ACC, the constitutional complaint may be admitted if a conflict with the Fundamental Law significantly affects the judicial decision, or the case raises constitutional law issues of fundamental importance. In view of all these aspects, the Constitutional Court considered it a question of fundamental constitutional importance in the present case to examine whether the interpretation of the law contained in the contested judgements, in the context of Article VI (3) and (4) of the Fundamental Law invoked in the petition, had regard to the fundamental rights aspects of the case in the context of the constitutional content of the right to the protection of personal data and the powers of the petitioner.

[24] On the basis of the above, the Constitutional Court examined the merits of the constitutional complaint, applying section 31 (6) of the Rules of Procedure, without conducting the admission procedure.

IV

[25] The constitutional complaint is well-founded according to the following.

[26] 1. The high level of protection of personal data was ensured by the previous constitution, the Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest, and the case-law of the Constitutional Court. In the Decision 1034/E/2005 AB, the Constitutional Court stressed that the condition for the right to the protection of personal data to be restricted and also its "main guarantee is the purpose limitation of the processing, i.e. its constitutionally justifiable nature", in relation to which the Constitutional Court also considered the existence of the former Data Protection Commissioner and judicial control as forms of guarantee. It also

interpreted the right to the protection of personal data as a right to informational self-determination, whereby each individual has the right to decide how his or her personal data is used. The protection of personal data has been upheld by the Fundamental Law, and an independent authority governed by a cardinal Act has been established to monitor and promote it. Following the entry into force of the Fundamental Law, the Freedom of Information Act also established and designated the National Authority for Data Protection and Freedom of Information as an authority under Article VI (4) of the Fundamental Law.

[27] The Minister of Justice pointed out that by the Act VI of 1998 "Hungary ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981 (hereinafter referred to as the Convention). By adopting the Act LIII of 2005, it also ratified the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed at Strasbourg on 28 January 1981, on supervisory authorities and transborder flows of personal data, signed at Strasbourg on 8 November 2001 (hereinafter referred to as the Additional Protocol), which is linked to the Convention and establishes data protection supervisory authorities. Since joining the European Union, Hungary has had to comply not only with its previous domestic and international legal obligations, but also with obligations under EU law. On the one hand, Article 16 (1) of the Treaty on the Functioning of the European Union and Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter: "Charter"), like the Fundamental Law, explicitly protect the right to the protection of personal data."

[28] In 2016, the EU co-legislators adopted the GDPR, "which has brought about a high degree of legal harmonisation in the protection of personal data in the European Union. This legislative harmonisation at regulation level has also meant that EU Member States have had to carry out a systemic review of their domestic law in order to give priority to the provisions of the GDPR and to facilitate its implementation. With the adoption of the Act XXXVIII of 2018 on the amendment of the Freedom of Information Act in connection with the data protection reform of the European Union and other related acts, the Hungarian law-maker has made adjustments to the general (horizontal) rules and the Act XXXIV of 2019 on the amendments to the Act necessary for the implementation of the data protection reform of the European Union, thus facilitating the implementation of the GDPR (and the data protection reform package). Due to the legislative amendments, the system of the Freedom of Information Act has also undergone a fundamental revision, thus according to section 2 (3) of the Freedom of Information Act, the Act – from 26 July 2018 – is applicable as a »code« (in its entirety) only for the processing of personal data for law enforcement purposes and – outside the scope of EU law – for national security and defence purposes, while section

2 (2) of the Freedom of Information Act designates the provisions that need to be applied in addition to the GDPR, i.e. to supplement it. These rules essentially relate to the operation and procedures of the Authority, and to a lesser extent to provisions that differ from or supplement the GDPR, which the GDPR otherwise expressly allows for. Both the legal consequences under domestic law, including the requirements under EU law, and obligations under international law aim to ensure effective protection of personal data. In this framework, both the GDPR and the Freedom of Information Act – in the data protection relationships falling within their scope – and the Convention establish the effective enforcement of the right to information self-determination with provisions at the level of principles."

[29] The principles should apply at all times to the processing of personal data, irrespective of the controller, the nature of the processing, the will of the data subject, his or her statements or any other circumstances. Supervisory control of the right to the protection of personal data is provided for by the Fundamental Law, Article 8 (3) of the Charter and Article 51 of the GDPR. According to Article 57 (1)(a) of the GDPR, which is directly applicable, the national supervisory authority shall monitor and enforce the application of the GDPR on its territory, and in this framework shall enjoy the powers under Article 58. The remedial powers under Article 58 (2) of the GDPR also extend to the possibility for the data protection supervisory authority to instruct the controller to "bring its processing operations into conformity" with the GDPR, and to order the erasure, rectification or restriction of personal data. Although the GDPR provides Member States with a general and common framework for the protection of personal data, it does not, despite its regulatory form, specify the form or detailed procedural framework for supervisory authorities, which is left to the Member States [Recital 151 of the GDPR]. Under Article 51 (4) of the GDPR, Member States are also required to notify their rules on supervisory authorities to the Commission by means of a special notification, which allows the monitoring of national solutions and their compatibility with EU law.

[30] According to Article 1 (2) (a) of the Additional Protocol, the powers of the supervisory authorities include the power to investigate and intervene. Pursuant to the so-called Explanatory Report to the Additional Protocol, supervisory authorities have two types of powers – investigative and intervening – which can be regulated by the parties in a number of ways, including the possibility to confer on the supervisory authority the power to decide, at its discretion, whether to require the controller to rectify or erase the data. In the interpretation of the Convention and the Additional Protocol, the provisions enabling the supervisory authorities to intervene effectively and enforce the principles are explicitly mentioned. On the basis of the Explanatory Report, the powers of the supervisory authorities in relation to the Convention and the Additional Protocol are not limited, i.e. the Parties may confer on their authorities any

additional powers that will make the supervisory function under the Convention and the Additional Protocol effective.

[31] Under the Freedom of Information Act, the Authority may carry out two types of procedures in the field of data protection. Investigation on the one hand, and the data protection authority's procedure on the other. On the basis of section 52 (2) of the Freedom of Information Act, the Authority's investigation does not qualify as an administrative authority procedure, it is basically an instrument of ombudsman-type legal protection, while the procedure of the data protection authority is an administrative authority procedure with the coercion, sanctions and guarantee system that is characteristic of it. The common element of the two types of proceedings is that they can be initiated both on request and ex officio, and they are complementary, therefore the Authority's investigation may be followed by a data protection authority procedure under the Freedom of Information Act. The aim of both procedures is to identify and remedy a possible violation of rights. In the investigation under the Freedom of Information Act, since the Authority's investigation is not based on EU law, the Authority may call on the infringing controller to remedy the infringement or to eliminate the imminent threat thereof, in accordance with section 56 (1) of the Freedom of Information Act. However, in the data protection authority procedure, given that the specific powers of investigation and rectification are determined by EU law, the Freedom of Information Act refers back to the provisions of the GDPR, which is directly applicable, instead of repeating the specific rules. As regards the specific legal consequences, Article 61 (1) (a) of the GDPR applies the codification solution by reference, according to which the Authority may apply the legal consequences set out in the GDPR in connection with the data processing operations specified in Article 2 (2) and (4) of the GDPR.

[32] Prior to the European Union's data protection reform, the provisions of the Freedom of Information Act in force until 29 June 2018 also allowed the Authority to require the controller to remedy the breach of rights within the framework of the investigation, or to establish the fact of unlawful processing within the framework of administrative authority proceedings, to order the erasure, blocking or destruction of unlawfully processed data, or to prohibit processing. The Freedom of Information Act did not previously distinguish between the powers of the Authority with regard to whether the given procedure was initiated at the request of the data subject or ex officio, therefore the Authority could apply the above legal consequences regardless of the initiator of the procedure.

[33] Until the amendment of the Freedom of Information Act due to the GDPR (29 June 2018), the data protection authority procedure initiated by the Authority was considered an *ex officio* procedure under section 60 (3) of the Freedom of Information Act, even if it was preceded by an investigation procedure initiated at the request of

the data subject. Thus, under the previous system of legal protection, the public authority (or the commissioner who had previously exercised public authority) had a clear and unambiguous possibility to conduct certain proceedings *ex officio* and to apply any legal measures it deemed necessary at its discretion.

[34] With the start of the application of the GDPR – in the light of Article 77 of the GDPR – the legislator had to ensure that the data protection authority procedure could be initiated not only *ex officio*, but also upon request, by extending the level of protection of the Freedom of Information Act. Section 60 (1) of the Freedom of Information Act clearly states that the Authority shall initiate the procedure of the data protection authority upon the request of the data subject, and may also initiate the procedure *ex officio* as a supplementary measure. Thus, the amendments to the Freedom of Information Act in the context of the implementation of the GDPR have extended and – in addition to the possibility to initiate an investigation – also provided effective legal protection for data subjects by granting them the possibility to initiate an administrative procedure. However, this change, i.e. the mandatory opening of the data protection authority procedure upon request, does not prevent the Authority from continuing to open an investigation or administrative procedure against the data controller involved in the breach in order to protect data subjects. In addition, in both *ex officio* and on-request procedures, it will examine the processing in general and in its entirety, even in the light of the other data subjects who are not otherwise aware of the processing or its unlawfulness.

[35] The reply of the Minister of Justice also indicated that the Government is not entitled to interpret the legislation authentically. However, in her professional view, the commissioners' regime based on the EU Directive legislation [Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data] and the authority regime between 2012 and 2018 were consistent that data protection supervisory authorities have a wide range of tools to use to stop unlawful processing, and this is also clear under the GDPR-based regime. All provisions of the GDPR have the basic aim of keeping personal data processing within a lawful framework, which can be based on the enforcement of the principles.

[36] Under Article 57 (1) (a) of the GDPR, the data protection supervisory authority is responsible for enforcing the application of the GDPR. Under Article 58 (2) of the GDPR, the data protection supervisory authorities are also empowered, in the context of the remedies granted to them, to warn, reprimand, prohibit unlawful processing or order the controller to bring its processing into compliance with the GDPR. Data protection compliance may be achieved in some cases by minor corrections (informing the data subject or changing the legal basis, etc.), but in other cases – specifically where the processing relationship is necessarily inherently at odds with the GDPR and the data

processing principles – the only way to bring the processing into compliance with the GDPR is for the controller to delete irretrievably and without delay the data it has unlawfully processed. If data protection supervisory authorities could not take action in their procedures against data processing operations that violate the GDPR – or the principles –, they would fail to protect not only the complainant in the case, but also other data subjects who might otherwise be affected by the unlawful processing. The work of data protection supervisory authorities would be rendered redundant if they could only intervene in cases of data subjects who have explicitly requested it before the supervisory authority. If the procedural discretion of data protection supervisory authorities were to depend on the enforcement of rights by data subjects, this would also prevent the authorities' main task of enforcing the GDPR (including the detection of data processing that violates the principles).

[37] Data protection supervisory authorities have the duty to investigate and enforce the application of and compliance with the GDPR within their own powers, acting independently (either upon request or *ex officio*). It would result in discrimination if in the case of data processing falling within the scope of the Freedom of Information Act – in the fields of law enforcement, national security, defence [see section 2 (3) of the Freedom of Information Act] – the Freedom of Information Act expressly allowed the Authority to erase data *ex officio*, while in the case of unlawful data processing falling within the scope of the GDPR the Authority would have to refrain from erasing unlawfully processed data. In this context, the Minister of Justice referred to a fictitious example: "in the case of the unlawful processing, in breach of the principles and with respect to a multitude of data subjects, of special data referred to in Article 9 of the GDPR [data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, or criminal personal data under section 5 (7) of the Freedom of Information Act], the Authority would not be able to act – in line with this interpretation – in the interests of the large number of data subjects, and the controller would only have to cease unlawful processing of data in respect of the data subjects who apply for this with the controller." Although in such a case the authority could decide to impose a fine under the GDPR, it still could not order the erasure of the data.

[38] If the Authority could not decide ex officio, in the absence of an explicit request by the data subject, on the erasure of unlawfully processed data, this would deprive the Authority of its substantive legal protection function derived from Article VI (4) of the Fundamental Law, and would significantly reduce, or even empty out, the high level of protection of the right to informational self-determination guaranteed by Article VI (3) of the Fundamental Law, which has been maintained for decades. Under such a provision of Member State law, Article 80 of the GDPR also allows for the possibility for organisations representing the data subject to act in the interest of the data subject,

even in the absence of a mandate from the data subject. The scope of criminal law protection also goes beyond the interests of the individual data subject [the offence of misuse of personal data under Article 219 (1) of the Act C of 2012 on the Criminal Code]. Article 79 of the GDPR also allows the data subject to have recourse to the data protection supervisory authority and directly to a court. Section 23 (5) (a) and (b) of the Freedom of Information Act also empowers the court to order the controller to "cease the unlawful processing operation" or "restore the lawfulness of processing", irrespective of the fact that the action may be brought by the data subject.

[39] The GDPR – as an act of Union law – can be interpreted by supervisory authorities and courts, but the right to provide an authentic interpretation is vested on the European Union's data protection authority and the Court of Justice of the European Union, whose case-law is binding on the data protection supervisory authorities and the courts as well. For such questions of EU law, it is the body with the authority to give an authoritative and definitive interpretation that can provide a final and reassuring answer, which would also make the matter clearly open to decision by the domestic courts from an EU law perspective. At the same time, the Authority's legal toolbox, the possibility to act in the interests of data subjects, can be derived not only from the GDPR, but also from the Fundamental Law. The law-maker has made it clear in the reasoning attached to the legislative amendments implementing the GDPR that it must refrain from legislating contrary to EU law, which also means that the complementary interpretation of the law deducted from the Fundamental Law and maintaining the level of protection derived from it, is not otherwise contrary to EU law.

[40] The Parliament adopted the Amendment Act on 9 November 2021, Chapter 10 of which also provides for the amendment of the Freedom of Information Act. Section 65 of the Amendment Act makes it clear that the Authority may apply the legal consequences set out in the GDPR in its decision delivered in the data protection authority procedure (with regard to processing to which the GDPR applies), in particular, upon request or *ex officio*, order the erasure of unlawfully processed personal data in the manner specified by the Authority, or otherwise restrict processing temporarily or permanently. According to Section 129 (2) of the Amendment Act, the amendment to the Freedom of Information Act entered into force on 1 January 2022.

[41] 2. The European Union has its own legal system based on international treaties, according to which the Union law is directly applicable in the territory of the Member States and it may also directly create rights and obligations for the subjects of law {Decision 2/2019. (III. 5.) AB (hereinafter: CCDec 1), Reasoning [17]}.

[42] The Constitutional Court has already stated in the Decision 2/2019. (I. 23.) AB that the binding force of European Union law does not arise by itself, but it is based on Article E) of the Fundamental Law and it does not overwrite Article R (1) of the

Fundamental Law, according to which the Fundamental Law shall be the foundation of the legal system of Hungary {Decision 11/2020. (VI. 3.) AB, Reasoning [54]}.

[43] "In most cases the parallel systems of Union law and the domestic norms do not cause any constitutional dilemma as the two normative systems are based on a common set of values. Article Q of the Fundamental Law and its special Article E on the Union law both require, as a constitutional obligation, compliance with the international law and with the Union law, the resolving of any collision is possible by paying respect to constitutional dialogue. In this respect [...] »the authentic interpretation of the founding and amending treaties of the European Union and of the so-called secondary or derivative law adopted on the basis of the foregoing – regulations, directives and other norms of EU law [...] fall under the competence of the European Court of Justice.« It does not mean that only the Court of Justice of the European Union may interpret the Union law as it needs to be interpreted for example by the Member States' courts that must enforce the Union law as well as by other subjects of the procedures. Similarly, it follows from Article 24 (1) of the Fundamental Law that the genuine interpreter of the Fundamental Law is the Constitutional Court. It does not prevent, however, other domestic and international organs, courts or institutions from interpreting the Fundamental Law or the laws of Hungary in the course of their own procedures. For example, according to Article 28 of the Fundamental Law, all courts shall provide an interpretation in conformity with the Fundamental Law, but this interpretation may not deter from the authentic interpretation practice of the Constitutional Court." (CCDec 1, Reasoning [35])

[44] "It should be supposed that both the Union law and the national legal system based on the Fundamental Law aim to carry out the objectives specified in Article E (1). With regard to the above, »the creation of European unity«, the integration, sets objectives not only for the political bodies but also for the courts and the Constitutional Court, defining the harmony and the coherence of legal systems as constitutional objectives that follow from »European unity«. To achieve the above, the laws and the Fundamental Law should be interpreted – as far as possible – in a manner to make the content of the norm comply with the law of the European Union." (CCDec 1, Reasoning [37])

[45] "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." {Decision 3212/2020. (VI. 19.) AB (hereinafter: CCDec 2), Reasoning [43]}

[46] 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 (cp. CCDec2, Reasoning [44]).

[47] Part of the protection of privacy is the right to the protection of personal data, which is contained in Article VI (3) of the Fundamental Law and which the Constitutional Court has understood as a "right of informational self-determination" since the Decision 15/1991 (IV. 13.) AB (ABH 1991, 40, 44 to 57, reinforced among others by CCDec 2, Reasoning [45]). The Fundamental Law, just as the Constitution, includes the concept of the "protection of personal data", which is explicitly considered a fundamental right {Decision 11/2014. (IV. 4.) AB, Reasoning [55], see also in this respect: Decision 3171/2017. (VII. 14.) AB, Reasoning [32], cp. CCDec 2 Reasoning [46]}.

[48] Thus, the right to the protection of personal data means that everyone has the right to decide about the disclosure and use of his or her personal data. Hence, approval by the person concerned is generally required to register and use personal data; the entire route of data processing and handling shall be made accessible to everyone, i.e. everyone has the right to know who, when, where and for what purpose uses his or her personal data. [...] Adherence 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. Each phase of data processing must comply with the notified and authentically recorded purpose. It follows from the principle of adherence to the purpose that collecting and storing data without a specific goal, »for the stock«, i.e. for unspecified future use is unconstitutional." {Decision 15/1991. (IV. 13.) AB, ABH 1991, 40, 42., reinforced among others in Decision 3110/2013. (VI. 4.) AB, Reasoning [50]}

[49] In the present case, the Constitutional Court therefore finds, bearing all of this in mind and taking into account the professional position of the Minister of Justice, that the petitioner is an independent authority established by a cardinal Act under Article VI (4) of the Fundamental Law, whose task is to monitor the exercise of the right to the protection of personal data and the right to access data of public interest under the Fundamental Law. The interpretation of the law contained in the challenged judicial decisions affects the operation of the petitioner in the context of the exercise of its powers, taking into account the provisions of the Fundamental Law, the GDPR directly applicable in the Member States of the European Union, as well as the regulations under the ACC and the Freedom of Information Act.

[50] 3. The GDPR provides for the establishment of an independent body of the Union, the European Data Protection Board (hereinafter: "Board"), to ensure the consistent application of the GDPR and to promote cooperation between supervisory authorities in the European Union. According to its Statutes, the Board is a body of the Union having legal personality and acting independently in the performance of its tasks or in the exercise of its powers. The Board will therefore ensure consistent application of the GDPR [Articles 1 and 2 of the Statutes], and the GDPR stipulates that the Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union [Recital 139 of the GDPR].

[51] The Constitutional Court noted after the submission of the petition that the petitioner had applied to the Board for an interpretation of the powers under Article 58 (2) (g) of the GDPR. In its Opinion No 39/2021, adopted on 14 December 2021, the Board took a position on the question whether Article 58 (2)(g) of the GDPR can serve as a legal basis for the supervisory authority to order the erasure of personal data ex officio, even in the absence of a request to that effect by the data subject. The Board therefore had to assess whether the powers of the supervisory authorities under Article 58 (2) (g) GDPR apply also in the absence of a request for erasure by the data subject. In the Board's view, Article 17 of the GDPR defines two independent categories of cases: erasure at the request of the data subject and erasure as a separate obligation of the controller. The latter power should be interpreted, on the basis of the Board's reasoning, as meaning that Article 58 (2) (g) of the GDPR provides an appropriate legal basis for the supervisory authority to order *ex officio* the erasure of unlawfully processed personal data in cases where no such request has been made by the data subject.

[52] In the context of the relevant amendment to the Freedom of Information Act which entered into force on 1 January 2022, the reasoning of the Amending Act makes it clear that in the course of the supervision of data processing operations subject to the GDPR,

"the National Authority for Data Protection and Freedom of Information may apply any of the legal consequences set out in this regulation, which is directly applicable and enforceable in Hungarian law, and highlights the most significant ones of these legal consequences by way of example, on the basis of which it may, either upon request or in the case of *ex officio* proceedings, order the erasure of unlawfully processed personal data, specifying the method of erasure in the light of the circumstances of the specific case, and may also temporarily or permanently restrict in any other way any processing operation unlawfully carried out by the controller."

[53] "According to the consistent judicial practice of the Constitutional Court, on the basis of a constitutional complaint based on section 27 of the ACC, it shall examine the compatibility with the Fundamental Law of the interpretation of law found in the judicial decision, i.e. whether the court enforced the constitutional content of the rights granted in the Fundamental Law. If the court acts without paying due attention to the fundamental rights affected by the relevant case and if the interpretation of the law developed by the court is not compatible with the constitutional content of this right, then the adopted judicial decision is contrary to the Fundamental Law.

At the same time, in its adjoining decisions the Constitutional Court also explained that it may not distract the power of the adjudicating courts to comprehensively assess the elements of the facts of the cases before them, it may only review whether the interpretation of the law underlying the weighing was in compliance with the Fundamental Law, and whether the constitutional criteria of weighing were complied with.

The Constitutional Court has already pointed out in a number of decisions that the State has an active duty to protect fundamental rights [Article I (1) of the Fundamental Law]." (CCDec2, Reasoning [27] to [29])

[54] The GDPR lays down as a matter of principle that the protection of natural persons with regard to the processing of their personal data is a fundamental right. The Constitutional Court, taking into account the opinion No. 39/2021 of the Board as a body of the European Union, and having regard to the provisions of the Fundamental Law and the regulation under the Freedom of Information Act, established that the interpretation of the law contained in the contested judicial decisions, according to which the petitioner – in the absence of powers – is not entitled to order *ex officio* the erasure of unlawfully processed personal data, is not in line with the position of the Board, which is responsible for ensuring the consistent application of the GDPR in the EU. Furthermore, the judicial decisions are inconsistent with the content of the fundamental right to the protection of personal data, as demonstrated and elaborated by the Constitutional Court in its case law and the regulations under the Freedom of

Information Act, which the legislator adopted to facilitate a uniform interpretation of the law, giving priority to EU law, as previously explained by the Minister of Justice.

[55] The Budapest-Capital Regional Court held that – with due account to the CILFIT criteria – the case did not raise a substantial question requiring the interpretation of EU law. The provisions of the GDPR applicable to the case were clear and the dispute could be resolved on that basis. Neither the Curia nor the Regional Court saw any reason to initiate a preliminary ruling procedure before the Court of Justice of the European Union on the final interpretation of the GDPR as an EU legal act.

[56] The Constitutional Court points out that the courts, in their decisions and deliberations in the context of the right to the protection of personal data – which is one of the independent fundamental rights –, failed to recognise that the broad supervisory control of data protection authorities had also been guaranteed under the Fundamental Law, EU law and obligations under international law prior to the GDPR. The Authority has a duty under the Fundamental Law to monitor the fundamental right to the protection of personal data. It exercises this control (constitutional duty) through its powers laid down in the cardinal Act. The purpose of the monitoring is to ensure that personal data are protected during each processing operation. If the Authority finds during the inspection that the processing of personal data by the controller is unlawful, it follows from the effective protection of fundamental rights, which is the main task of the Authority, that it may not only inspect and detect unlawful personal data processing, but also order the erasure of such data ex officio (in order to protect the fundamental rights of third parties). Otherwise, in the absence of effective protection of fundamental rights, both the powers and the exercise of constitutional functions are limited. The protection of personal data is a "fundamental right of a protective nature", which requires effective legal protection by public authorities. On the basis of Article E (2) and (3) and Article VI (4) of the Fundamental Law and the GDPR as EU legislation ensuring the uniform application of data protection and freedom of information, the Authority is entitled to order the erasure of unlawfully processed personal data *ex officio*, even in the absence of a request to that effect.

[57] 4. Based on the above arguments, the Constitutional Court established that the judgement No. Kfv.II.37.001/2021/6 of the Curia and the judgement No. 105.K.706.125/2020/12 of the Budapest-Capital Regional Court were contrary to the Fundamental Law and, therefore, annulled them. The Constitutional Court, in accordance with its consistent case-law, did not examine the possible violation of other provisions of the Fundamental Law invoked in the petition with regard to the annulment of the challenged court decisions.

[58] After the annulment of the court decisions, the procedural means of remedying the constitutional complaint shall be determined by the Curia on the basis of the

decision of the Constitutional Court and with the proper application of the relevant procedural rules.

Budapest, 01 March 2022.

Dr. Tamás Sulyok,
President of the Constitutional Court
rapporteur

Dr. Tamás Sulyok, President of the Constitutional Court on behalf of Justice *dr. Egon Dienes-Oehm* unable to sign

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

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

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

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

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

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

Dr. Tamás Sulyok, President of the Constitutional Court on behalf of Justice *dr. Ildikó Hörcherné dr. Marosi* unable to sign

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

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

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

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