Presentations given at the international conference organised to mark the 30th anniversary of the Hungarian data protection institutional system (abridged summary)

Venue: NAIH headquarters (Budapest, District V, Falk Miksa u. 9-11.)
Ceremonial Hall
Host of the Conference: Dr Júlia Sziklay

I. Morning session – International Part (in English)

Ms. Júlia Sziklay, Vice President for International Relations of National Authority for Data Protection and Freedom of Information opened the conference celebrating the 30th anniversary of the Hungarian data protection institution.

Mr. Attila Péterfalvi, President of National Authority for Data Protection and Freedom of Information greeted the President of Hungary and the President of the Constitutional Court, all guests who joined the conference. He expressed his greetings to the representatives of the international diplomacy attending the session, and pointed to the fact that in addition to celebrating the 30th anniversary another reason of the present conference is that Hungary is the host of the meeting of the Central European Data Protection Authorities this year. He has also taken the opportunity to congratulate to the 45th anniversary of the Austrian Data Protection Authority, and declared that a joint celebration of the Hungarian and the Austrian authorities would take place in October 2025 in Brussels. On the occasion of the Hungarian anniversary Mr. Attila Péterfalvi remembered to Mr. László Sólyom, former President of Hungary, who was also the founder of the Hungarian data protection regulation, and played a particularly active role in the field of data protection and freedom of information.

Mr. Tamás Sulyok, President of Hungary welcomed all who attended this international conference organized on the occasion of the 30th anniversary of the Hungarian data protection institution. He emphasized that personal data can directly derived from the principle of human being. Self-determination shall ensure that fundamental rights are protected, under the concept of the rule of law. The regime change in Hungary was not only a political change, but it signified a break with the past that denied human autonomy. Constitutional rules have been established to govern the rules of storage of data. With the access to internet a new world of access to data has been created, and the right to informational self-determination has become

more vulnerable than ever. The European Data Protection Board contributes to the process of strengthening the law of data protection. Modernisation must not undermine human being. The enforceability of data protection rights also raises several questions, it reflects the effectivity of the instruments protecting human rights. Emerging new technology, the use of AI change the world, mutual understanding of the rules is crucial, and the law can never lose morality.

Mr. Péter Polt, President of the Constitutional Court emphasized in his presentation that according to the fundamental law everyone has the right to the protection of personal data and freedom of information. Information rights in Hungary should be given priority in fundamental law, today these rights are protected by an independent authority. The institution of data protection is now celebrating its 30th anniversary, for this occasion he pointed to the connection points between the Data Protection Authority and the not much older Constitutional Court. The institutional context is essential for the protection of information rights due to the fact that under the catalogue of the fundamental rights the Constitutional Court also protects the right to data protection. The guidelines and the dogmatic of the fundamental law is very consistent. As an example among others he mentioned a decision of the Constitutional Court in the field of the protection of personal data, namely Decision 15/1991 (13.04) of the Constitutional Court on the use of personal data and the personal identification number which declared that in the absence of a definite purpose and for arbitrary future use, the collection and processing of personal data is unconstitutional. European rules on data protection have also provided to increased data protection. Mr. Péter Polt also mentioned the name of László Sólyom as the first President of the Constitutional Court, who laid down the foundation of the Constitutional Court's practice.

* **

Presentations:

Role of the EDPB and the importance of cooperation among data protection authorities

by Mr. Zdravko Vukić, Deputy Chair of the European Data Protection Board (EDPB), Director of the Croatian Personal Data Protection Agency

The lecturer pointed out that having strong co-operation with the Hungarian Data Protection Authority, he feels being with colleagues, unified by common history. He emphasized the importance of co-operation between data protection authorities. The presentation explained that The European Data Protection Board (EDPB) is an independent European body with legal personality. It ensures that the General Data Protection Regulation and the Law Enforcement Directive are applied consistently. The EDPB promotes effective cooperation among data protection authorities throughout the European Economic Area (EEA). EDPB is composed of the heads of the national data protection authorities of the countries in the European Economic Area, as well as the European Data Protection Supervisor (EDPS). The data protection authorities are responsible for enforcing data protection law at a national level and at a cross-border level by cooperating through the one-stop-shop mechanism. The EDPB takes binding decisions on cross-border cases on which no consensus is reached. Data protection authorities have dual responsibility: enforcement at national level and co-operation at international level. EDPB provides legal certainty, consistent application of the GDPR across the European Union. In 2024-2025 the EDPB continued to provide guidance on key issues, the purpose of the guidelines is the proper implementation of the GDPR. As examples he mentioned development of information for children, practical information designed for SMEs as these companies still face difficulties in the application of the GDPR, raise awareness in data protection. The virtual assistance developed for GDPR compliance is called OLIVIA and is available in English, Croatian and Italian – other languages will be added in the future – at https://olivia-gdpr-arc.eu/en. Consistency opinions of the EDPB based on Article 64 GDPR are non-binding opinions reinforcing a common enforcement culture. He highlighted Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms adopted on 17 April 2024, and Opinion 24/2024 on certain data protection aspects related to the processing of personal data in the context of AI models adopted on 17 December 2024. The role of EDPB is to provide guidance on interplay between GDPR and new EU digital laws, monitor and assess new technologies, including AI, to promote human-centric approach, secure inter-regulatory co-operation. The EDPB also contributes to the global dialogue on data protection.

Freedom of Information in Austria and the role of the Austrian DPA

by Mr. Matthias Schmidl, Head of the Austrian Data Protection Authority

The presentation explained the relation of data protection and freedom of information in Austria. The historic background of data protection goes back to the 1980s, the data protection act was adopted in 1978, and entered into force in 1980, also the Data Protection Commission was established in this year. In 1981 Austria signed, in 1988 ratified the Convention 108. Austria joined in 1995 to the European Union, in 2000 the new Data Protection Act entered into force. The Data Protection Commission remained until 2014, when it was replaced by the Data Protection Authority. As far as freedom of information is concerned, it has no tradition, this is a new territory in Austria. Based on Article 20 (3) of the Austrian Constitution, the rule of official secrecy governed since 1925, the duty to grant information applies since 1988, but this did not create a subjective right for the individual. More liberal jurisprudence of the Constitutional Court and the Supreme Administrative Court concerning duty to grant information, based on jurisprudence of the European Court of Human Rights on Article 10 of the European Convention on Human Rights, resulted in granting subjective right to information in certain cases, i.e. to public watchdogs. The act on freedom of information and the amendment of the Constitution was adopted in 2024. In the Constitution subjective right to freedom of information vis-à-vis administrative authorities and public bodies, also duty to proactive publication of information of general interest of administrative authorities and courts have been declared, with the following exceptions: for compelling reasons of European integration or foreign policy, in the interest of national security, in the interest of national defence, in the interest of maintaining public order and security, in the interests of the unimpaired preparation of any decision, to prevent significant economic or financial damage to the bodies, territorial authorities or other self-administering bodies, in the overriding legitimate interest of another person. The lecturer also explained the procedure of requesting information and legal remedies.

Interplay between Freedom of Information and Data Protection from the Czech perspective

by Mr. Petr Jäger,Vice-President of the Office for Personal Data Protection, Czech Republic

In the presentation delivered, both rights at stake were viewed as concurrent and often conflicting. Although the Freedom of Information Act (FOIA) was introduced in the Czech Republic at approximately the same time as the establishment of the

Czech Data Protection Authority (DPA)—the FOIA in 1999 and the previous Act on Personal Data Protection in 2000—the Czech DPA became specifically engaged with this topic much later, in 2020.

The legislator recognized that after 20 years, no central authority was responsible for the consistent application and interpretation of the FOIA, as the Ministry of the Interior had a limited role in this field. Consequently, in 2020, some decision-making powers were transferred to the Czech DPA; however, this was done, again, without granting it the general competence of a central authority.

Three levels of administrative decision-making now exist: (1) a public entity as the first instance, (2) the Czech DPA in some cases or regular administrative authorities as the second instance, and (3) the Czech DPA as an extraordinary review authority also responsible for inactivity protection.

Although the GDPR does not represent a fundamental revolution in the substantive protection of personal data, the relationship between the FOIA and the GDPR remains unresolved. Article 86 of the GDPR calls for the reconciliation of public access to official documents with the right to personal data protection; however, the Czech FOIA in its Section 8a para. 1 provides a loop reference to the GDPR.

The presentation addressed inconsistencies in classifying the appropriate legal basis under the GDPR. It concluded that the Czech FOIA—when applied to the disclosure of information upon request—meets the criteria of Article 6(1)(e), as it involves a task carried out in the public interest. Article 6(1)(c) — the legal obligation basis — is also applicable in the FOIA context, but typically in situations where the law mandates proactive publication of information without any (administrative) procedure. By contrast, the presentation excluded the possibility of performing the very same public task based on the data subject's consent pursuant to Article 6(1)(a), as the public entity would act ultra vires, beyond its competence. It was noted that there has been a long-standing misconception regarding the supposed hierarchy of legal bases for data processing. Consent was traditionally viewed as the primary legal basis, with all other bases seen as mere exceptions to the duty to obtain consent.

In the context of developments in case law, the landmark decision of the Constitutional Court (no. IV. ÚS 1378/16) from 2017 was mentioned first. A previous judgment of the Supreme Administrative Court was overruled. The factual question concerned the extent to which public entities should disclose information on the salary of each public employee. The key message, which also aligns perfectly with the GDPR, is that all conflicting fundamental rights must be weighed in each individual case and a fair balance must be struck between them, since they are equivalent rights. In 2025, the Supreme Administrative Court challenged this approach again, stating that disclosing personal data about a public official or employee of the public administration that reveals his public or official activities is not subject to any proportionality test. The Czech DPA was not a party to this proceeding, was not even consulted, and has serious doubts about this approach.

Lastly, the presentation mentioned the judgment of the Court of Justice of the EU of 3 April 2025, C-710/23, "L. H. v Ministerstvo zdravotnictví," which was delivered upon a request for a preliminary ruling from the Supreme Administrative Court. The Czech court asked whether, in the context of the GDPR, it may maintain its pre-GDPR case law requiring public bodies

handling information requests to consult the data subject and allow their participation prior to disclosing personal data (which is, in general, perfectly appropriate). The reply from the CJEU was affirmative. However, surprisingly for the Czech DPA, the Czech court had not recognized that similar safeguards have already been embedded in the GDPR. The controller's duty to inform the data subject under Articles 13 or 14, combined with the data subject's right to object to the processing of personal data based on Article 6(1)(e) according to Article 21, delivers a safeguard very similar to the practice that was introduced long ago by national case law alone.

Development of Data Protection Legislation in Slovakia: Past, Present and Future Perspectives

by Ms. Ella Germuskova, expert of The Office for Personal Data Protection of the Slovak Republic

The constitutional foundation of the data protection regulation goes back to 1991. With Act No. 23/1991, the Federal Assembly of the Czech and Slovak Federative Republic enacted the Charter of Fundamental Rights and Freedoms, declaring also the right to informational self-determination. Article 10 (3) provided that „Everyone has the right to protection against unauthorised collection, disclosure, or other misuse of personal data“, which indicated a clear requirement for the adoption of a specific law on personal data protection. The Act No. 256/1992 on the protection of personal data in information systems was passed by the Federal Assembly of the Czech and Slovak Federative State on April 29, 1992. However, parliamentary elections in June 1992 triggered dramatic change of political landscape and initiated the process of dissolution of the federation. Constitutional Act on the Dissolution of the Czech and Slovak Federative Republic was enacted on November 25, 1992, and Czechoslovakia´s legal existence came to a close on December 31, 1992. Due to the dissolution of Czechoslovakia, Act No. 256/1992 became unenforceable, and there was an urgent need to adopt national legislation to fill in the legal gap left by the unenforceable federal act. The National Council approved the Act No. 52/1998 on personal data protection in information systems on February 3, 1998, but only partial compatibility with Directive 95/46/EC was achieved, when the law came into force on March 1, 1998. The government did not fulfill its role in establishing state supervision over the protection of personal data (according to § 26(1) of the Act) and thus, some parts of the law were unenforceable from the beginning, as there was no authority to execute it. This situation lasted until the appointment of a Plenipotentiary for the Protection of Personal Data on February 10, 1999. Primary driver for the following law was the strategic goal of joining to the European Union. The National Council of the Slovak Republic approved Act No. 428/2002 on February 20, 2002, and it came into force on September 1, 2002. It expanded the scope of data protection, strengthened the rights of individuals, and introduced more detailed obligations for data controllers. The most crucial contribution of Act No. 428/2002 was the creation of a fully independent supervisory authority - the Office for Personal Data Protection of the Slovak Republic. In 2018, Act No. 18/2018 was adopted to align the Slovak legal order with the GDPR and also transposed the Law Enforcement Directive (EU) 2016/680 for the police and justice

sectors. Practice has revealed significant structural problems with the 2018 law due to the "Dual-Track" System, meaning the duplication of the directly applicable GDPR text into national legislation, which caused legal uncertainty. The proposed 2025 reform aims to replace the single complex law with two separate, streamlined acts: 1) a new Data Protection Act, which will only contain provisions necessary for the application of GDPR in Slovakia, and 2) a separate law for law enforcement, which will be dedicated exclusively to the transposition of the Law Enforcement Directive (EU) 2016/680.

Building bridges – between access to public information, data protection and AI

by Ms. Jelena Virant Burnik, Information Commissioner, Republic of Slovenia

The Data Protection Authority was established in Slovenia on 31 December 2005 (Access to Public Information Commissioner in 2003), it will celebrate its 20th anniversary this year (AI Market Surveillance Authority will be established in 2026). Slovenia is signatory of the Tromso Convention.

In the field of access to public information, the Data Protection Authority is deciding on appeals under Access to Public Information Act and Media Act. It may instruct on which data must be disclosed or provided to journalists, return the matter back to the first instance body or uphold a decision.

The number of complaints is increasing (776 complaints and more than 370 information requests in 2024), there is a need for additional resources. The authority is building bridges between access to public information and data protection, to answer the questions when can (or must) the personal data be disclosed, in the case of employees in the public sector and public officials, also applying the public interest test. In the field of data protection, based on the 2024 annual report, there were 1650 supervision cases and 2580 consultation cases, and additionally many activity of raising awareness, and also the EDPB and international cooperation.

The cases cover video surveillance, unlawful disclosures, unlawful or excessive collection, direct marketing, poor security, inadequate information, access requests. The Commissioner also presented the new competencies under DSA, DGA, DA, AIA, the Interplay with digital agenda acts and AI Act, raising the question, how it will affect the guaranties under GDPR. Bridging the areas of Data Protection and AI, the authority is dealing with questions what is personal data/data under AI Act, in the context of anonymization and pseudonymization, and also with the definitions of data controller or developer. Market surveillance authorities for supervision of the AI Act are expected to be the Agency for Communication Networks and Services, the Information Commissioner, the Market Authority, the Bank of Slovenia, the Insurance regulator. When building a bridge between AI and access to public information area many questions will need to be answered: is the information is available in a materialized form, and if AI model can be considered public information. Is there personal data exemption – is the

AI model (truly) anonymized? Must business secret exemption be applied? Who are the parties of the procedures, is the public body a developer? Building all the three bridges between the areas of competence of the Information Commissioner will increase legal certainty and public trust.

II. Afternoon session – the history and status of information rights in Hungary (this part of the conference will be held in Hungarian)

Commemorative medal presentation

During the afternoon session of the conference, which focused on domestic law, Dr. Attila Péterfalvi presented the NAIH silver commemorative medal posthumously to Pál Könyves Tóth, the author of the first Hungarian draft law on information rights. The award was accepted by the daughter of Pál Könyves Tóth.

Attila Péterfalvi:

Thirty years of Hungarian data protection: three decades in the mainstream of development of European law, in a changing technological environment

In his presentation, the president of NAIH reviewed 30 years of data protection history. In connection with the presentation of the commemorative medal, he said that his presentation included a document that Pál Könyves Tóth had previously collected in the archives. Before giving his historical overview, he pointed out that the relationship between technological development and privacy is the most important issue today, with AI being the focus. He quoted the study of Warren and Brandeis, which argues that the appropriate solution is a new interpretation of the "right to privacy". With regard to the stages of data protection regulation, he recalled the first-generation legislation (in the 1970s in Western Europe, the consequences of computer technology development, data processing and data storage by the state on the privacy of citizens), and second-generation legislation (1980s-1990s, when legislation no longer focused on technology but on the person behind the data, the right to informational self-determination).). In third-generation legislation, during the period of EU enlargement and global technological trends, the emphasis shifted from the right to informational self-determination to the development of legal bases for data processing and the principle of fair processing, due to the volume and quality of information flows. With regard to the regulation of data processing in Hungary, the speaker mentioned Act V of 1973 on statistics, Act IV of 1977 on the amendment and consolidated text of Act IV of 1959 on the Civil Code of the Hungarian People's Republic, according to which computerised data processing may not infringe on personal rights. He presented documents from the correspondence between the Central Statistical Office and the Council of Ministers from the period when the information law was being prepared and the draft was being drawn up. The historical background at this time was perestroika (the economic and social reform package launched in the Soviet Union in 1985 to completely reorganise the economy) and glasnost (making the country's leadership transparent), the effects of which also spread to Hungary. He presented a photograph of an archival copy of the 1990 draft law on the processing of personal data and the disclosure of data of public interest (source: lecture of Pál Könyves Tóth on *The background of the Data Protection Act at the Hungarian Central Statistical Office based on archival documents*). He referred to decision no. 15/1991. (IV. 13.) AB of the Constitutional Court which established that a general and uniform personal identification number that can be used without restriction is unconstitutional, and stated that the right to the protection of personal data is not interpreted as a traditional right of protection, but rather taking into account its active side, as a right to informational self-determination. The draft law was submitted by the government to the Hungarian Parliament in the spring of 1992, which adopted Act LXIII of 1992 on the protection of personal data and the disclosure of data of public interest (Avtv) on 27 October 1992. The law came into force on 1 May 1993. The data protection commissioner should have been elected by 1 October 1993, but the ombudsman institution was finally established by the Parliament on 30 June 1995 with Resolution no. 84/1995. (VII.6.) OGY. A unique feature of the Act compared

to the European regulation was that, in addition to the protection of personal data, it also contained guarantees of freedom of information, a first in Europe, and entrusted the Data Protection Commissioner with the task of "safeguarding" both rights. Between 1995 and 2011, the tasks and powers of the Data Protection Commissioner, who was elected by the Parliament and reported exclusively to the Parliament, were defined by the Avtv. and Act LIX of 1993 on the Parliamentary Commissioner for Civil Rights.
His functions can be divided into three categories:
1) protection of fundamental rights (monitoring the enforcement of information rights, shaping the domestic and EU regulatory environment through opinions, interpreting legislation regulating data processing and promoting the enforcement of information rights)
2) ombudsman-type legal protection (investigating citizens' complaints, formulating recommendations and resolutions, informing the public)
3) enforcement of the law by public authorities (with an ever-expanding scope of competence; initially this only included supervision of classified data and the data protection registry, but from 2003, in preparation for EU accession, and then from 2005, with the amendment of the Avtv., the focus shifted increasingly to the transition into the role of public authority).
Act LXV of 1995 on State Secrets and Official Secrets supplemented the Commissioner's powers by stipulating that he or she "may initiate the narrowing or broadening of the types of data defined as state secrets and official secrets" and that "if, in the course of the data protection commissioner's proceedings, he or she considers the classification of the data to be unjustified, he or she shall call upon the classifier to change or revoke the classification." Act LXVI of 1995 on public records, public archives and the protection of private archival material amended the definition of data of public interest, broadening the scope of bodies covered by the Act. The concepts of processor and data processing were incorporated into law in 1999. In 1999, the European Union's Data Protection Working Party issued an opinion on Hungary's data protection provisions, and its assessment and recommendations were accepted by the European Commission in its decision of 26 July 2000. Hungary joined the European Union in 2000 in the field of data protection. In the spring of 1993, the Hungarian government signed the Council of Europe Convention No. 108 on data protection, which is the first legally binding international instrument adopted in the field of data protection concerning the protection of individuals with regard to automatic processing of personal data. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 was adopted in 1995, and Member States had to implement its provisions by 1998. On 1 May 2004, Hungary became a full member of the Working Party established by Article 29 of the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (an independent advisory body operating alongside the European Commission, composed of the data protection commissioners/authorities of the Member States). 1 January 2004 marked a new era in domestic data protection with the entry into force of the amendment to Act LXIII of 1992 on the protection of personal data and the disclosure of data of public interest, which was harmonised with the law of the European Union in connection with our accession to the EU. The traditional role of the ombudsman in the field of personal data protection changed. The data protection commissioner's tasks and powers were expanded. Pursuant to Article 16 of the transitional provisions of the Fundamental Law, the mandate of the incumbent Data Protection Commissioner ceased upon the entry into force of the Fundamental Law. Act CXII of 2011 on the Right of Informational Self-determination and on Freedom of Information (Infotv.) entered into force on 1 January 2012, under which the National Authority for Data Protection and Freedom of Information is responsible for

monitoring and supervising the enforcement of the right to the protection of personal data and the right to access data of public interest and data accessible on public interest ground. On 27 April 2016, the European Parliament and the Council adopted the new EU data protection package, two elements of which are the Regulation laying down a general framework for data protection (Regulation 2016/679/EU – GDPR) and the Directive on the protection of personal data processed for law enforcement purposes (Directive 2016/680/EU – the Law Enforcement Directive). While the GDPR is directly applicable throughout the EU from 25 May 2018, Member States had to transpose the Directive into their national legislation by 6 May 2018.

The tasks of the data protection authority with regard to the European Union's Digital Package:

- Based on all new EU regulations, the GDPR applies to the processing of personal data, regardless of the technology used, as has been the case to date, and data protection authorities are dealing with an increasing number of cases each year.
- Participation in the work of the European Data Protection Board, including the ongoing formulation of new guidelines, and, among other things, the new task of coordinating participation in the new EU digital bodies.
- In Hungary, performing the registration and supervisory tasks based on the Data Governance Act (DGA) and participating in the work of the European Data Innovation Board.
- The European Union Digital Data Strategy Department was established in 2024, and a new AI Laboratory will be established in 2025 alongside the Forensic Laboratory.

Indirect effects of AI and the new regulation:

- In matters concerning personal data, the AI Regulation leaves data protection powers independent of other authorities, and cooperation between AI and other authorities is expected to be necessary in many cases.
- In an AI test environment (sandbox), if personal data is also processed, it is mandatory to involve the data protection authority of the Member State concerned, and it is rare for an AI to be trained completely without personal data.
- In addition to the material and financial requirements, continuous training is necessary to adequately handle new tasks and challenges.
- The Authority also uses an AI-based solution to transcribe large amounts of audio recordings collected as evidence in certain cases (Alrite), with appropriate organisational and internal regulatory safeguards.

At the end of his presentation, the speaker presented the organisational structure and statistical data of the National Authority for Data Protection and Freedom of Information in terms of staff numbers and cases.

István Stumpf, former judge of the Constitutional Court:

The role of the two information rights in democratic public

At the beginning of his presentation, he emphasised the importance of the 30th anniversary, which is a very long period in a person's life and a significant milestone for a legal institution as well. The anniversary calls for reflection, and Attila Péterfalvi fulfilled this obligation in his presentation on the history of the data protection institution. The right to personal data protection is the citizen's "shield" against the state, which means that everyone has control over the use of their personal data. Without the protection of personal data, there is no freedom of expression or freedom of assembly. The right to access data of public interest is the citizen's "sword", which ensures the transparency of the state's operations and the possibility of monitoring power. The speaker contrasted the principles of 30 years ago with the functioning of today's digital world. The state and global corporations collect large amounts of data. The question arises as to how the logic of algorithms can be supervised and how the principle of transparency can be enforced. Similarly, information overload and deliberate disinformation, the phenomenon of "fake news" cause at least as much of a problem. Easily accessible public data from reliable sources provide citizens with a reference point that enables them to navigate the sea of false information independently.

Böszörményiné dr. Katalin Kovács, Vice-President of the Curia:

The Curia's approach to litigation concerning information rights

The number of lawsuits related to the disclosure of data of public interest is growing at the Curia, with 19 such lawsuits in 2021 and 134 in 2025. Citing the provision of the Fundamental Law, the speaker pointed out that the right to access and disseminate data of public interest is not an absolute right and may be constitutionally restricted under Article I (3) of the Fundamental Law. It is also a provision of the Fundamental Law that public funds are the revenue, expenditure and claims of the state (Article 39(3)). Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (Infotv) promotes the achievement of the objective set out in Section 1 by laying down provisions ensuring access to data of public interest against public bodies. In a lawsuit concerning the disclosure of data of public interest, the body or person performing a public task is the defendant.
With regard to the definition of a body performing public tasks, the speaker referred to a case from the practice of the Curia in which a decision had to be made, in connection with a request

for public data relating to the awarding of a prize by a body (issuance of a copy of a certificate), as to whether the body performed activities that qualified as public tasks and whether it handled data of public interest or data accessible on public interest grounds. According to the Curia's interpretation of the law, the body cannot be considered a body performing public tasks because it awards prizes to representatives of various legal professions on the basis of personal recommendations received, for the purpose of recognising their activities, it does not manage public funds, it does not handle data of public interest or data accessible on public interest grounds, and therefore, as an independent entity, it cannot be obliged to disclose such data. According to the case law of the Curia, an organisation performing public tasks can only be obliged to disclose data that actually exists and is handled by it; if the controller disputes the existence (handling) of the data, the requesting party is obliged to prove it. The burden of proof to verify the lawfulness and the reasons of refusal to comply with the request lies with the controller. However, in a dispute between the parties, this is preceded by the plaintiff having to prove that the requested data is processed by the defendant. A request for the disclosure of data of public interest can only be fulfilled by indicating the public source of the requested data if it is accessible to the requesting party and contains the information specified in the request in a concrete, unambiguous and comprehensive manner. According to the Infotv., it cannot be disclosed if it is classified data under the law on the protection of classified data or if the fundamental right is restricted by law for special purposes (Section 27(1) and (2)). Pursuant to Section 27(3) of the Infotv., it is not sufficient to refer to business secrets in general terms, without specifics, in a formal manner; the justification for the restriction must be demonstrated and proven. The mere reference that certain solutions are classified as business secrets, the disclosure of which would cause disproportionate harm because unauthorised persons could become aware of the details and thus have the opportunity to use them at a later date, does not justify the refusal. With regard to the framework of the litigation, the speaker stated that reasons other than those cited in the response given to the data request may be indicated, but the court may only examine the legality of the refusal in the context of the reasons for refusal raised in the defendant's counterclaim. With regard to the litigation, she also addressed the issues of deadlines and reimbursement of costs. In a lawsuit for the disclosure of data of public interest, the judgment ordering the disclosure of data must be clear, definite and enforceable. The mere assumption of the existence of data cannot serve as a basis for an obligation to disclose data in the absence of other evidence. The operative part of the judgment ordering the disclosure of data must specify the data to be disclosed with sufficient detail, and the grounds for the judgment must explain the legal and factual basis for the obligation to disclose the data.

With regard to the protection of personal data, the speaker emphasised its importance as a fundamental right, a fundamental right that limits freedom of information, an obstacle to the fulfilment of requests for data of public interest, and the reason for protection is based on the respect for privacy. The protection of personal data is expressly mentioned as a personal right in Section 2:43(e) of the Civil Code, and the EU legal background is the GDPR. On the question of what constitutes personal data, the Curia ruled that the plaintiff's name, occupation and address constitute personal data. According to the Curia, the fact that this data is also recorded by the Bar Association does not affect its status as personal data. In the specific case referred to, it had to be assessed whether or not this data had been misused by the defendant. In its decision based on Article 4(1) and (2) of the GDPR, the Curia ruled that an email address containing the full name of a natural person constitutes personal data. The Curia has stated in several decisions that the unlawful processing of personal data does not automatically result in a violation of personal rights, including the right to the protection of personal data set out in

Section 2:43(e) of the Civil Code. The Infotv. (and the GDPR), as well as the Civil Code, protect personality through the protection of personal data, but regulates it from a different perspective, with different scopes of protection, which is related to the different personal and material scope of the referenced legislation; a violation of personal rights must affect human dignity. The Curia ruled that a possible infringement of data protection rules does not automatically mean that the infringement also constitutes an unlawful interference with the privacy of the person concerned to such an extent that it also constitutes a violation of personality rights under the Civil Code. In this regard, the Curia referred to a case in which the plaintiff found that he was unable to comment on an article shared on one of the defendant's social media profiles and that his previous comments were no longer accessible. According to the Curia, invoking the right to freedom of expression as a fundamental right of communication alone – in the absence of a subjective right relating to personality rights – does not justify the application of the personality rights sanctions provided for in the Civil Code. A special situation arises when the disclosure and publication of personal data recorded in court proceedings is at issue. According to Constitutional Court Decision no. 3021/2018. (I. 26.) AB, the public nature of the courtroom constitutes a special type of publicity and is governed by the procedural rules applicable to the proceedings in question. The Curia has ruled that the disclosure to the press of the name and other personal data of the person subject to the proceedings is an exceptional possibility and requires individual discretion in each case. It may be justified primarily in cases where the criminal offence that is the subject of the proceedings is a violent crime or a crime involving a significant penalty for an item of outstanding value, therefore, it is of significant public interest. If there is no public interest in the disclosure of the data, the specific procedural rules governing the proceedings take precedence. In the present case, since the plaintiff did not give his consent to be identified and there was no interest that would have justified his individual identification, the right to information did not override the plaintiff's right to privacy, and therefore, in the context of reporting on the criminal proceedings, the presentation of the defendant in uniform, with his rank insignia and name tag, and the unedited publication of his final statement violated his personality rights. In another case, the plaintiff expressly refused to consent to the defendant publishing a statement containing his personal data in a publication presenting the wealthiest persons in the Hungarian economy. The Curia found that the defendant's data processing without the plaintiff's consent was necessary for the purposes of the legitimate interests pursued by the defendant – to exercise its fundamental right to freedom of expression – where such interests were not overridden by the interests or fundamental rights and freedoms of the plaintiff, and therefore the defendant's data processing was lawful. Also in a data protection lawsuit, the plaintiff requested that the defendant, a forensic psychologist appointed in the plaintiff's divorce proceedings, be ordered to disclose the results of psychological tests and documentation relating to the plaintiff. The right of access enables the data subject to obtain from the controller confirmation with regards to the accuracy and the lawfulness of the processing. In this case, it was important to determine whether the exercise of the right of access contributed to the achievement of the objective set out in recital (63) of the GDPR, which was not the case here.

Gergely Palotás, Budapest Metropolitan Court, Deputy Head of the Civil Division:

Judicial enforcement of rights in the field of freedom of information and data protection

The speaker began by saying that although he was giving his presentation on the occasion of an anniversary, he would nevertheless focus primarily on the present. His presentation was divided into two parts, covering both the judicial enforcement of freedom of information and data protection litigation.

I. In connection with lawsuits that can be brought in relation to requests for access to data of public interest, he briefly presented the new regulations, which aim to speed up the process of these lawsuits and increase their efficiency. A special, accelerated procedure similar to that of lawsuits concerning corrections in the press will apply. He criticised the fact that the acceleration is two-tiered, with only the proceedings of the court being accelerated and not the claimant. The dual deadline for filing a claim in proceedings before the Authority remains in place, which also works against efficiency. He pointed out that the awareness of the claimant (accuracy of data requests) and the public authority (ensuring effective legal remedy) is of paramount importance in the changed regulatory environment.

The presentation reviewed the most significant issues that have arisen in judicial practice in recent years.

1. The four-step public interest test developed by the Constitutional Court constitutes a deviation from the data principle in the exceptional case of closely related information elements. On this basis, the Curia ruled in one of its decisions that if the data (information elements) contained in the minutes that are the subject of the data request are so closely related that the separation of individual elements would result in meaningless data, it is not possible for the court to decide separately on the disclosure of individual parts of the document.

2. The possibility of initiating legal proceedings is limited by the fact that, pursuant to Section 27(3a) – (3b) of the Infotv., the law does not provide effective judicial protection for the data requester in the event of failure to comply with the obligation to provide information when entering into a financial or business relationship with a person belonging to a sub-system of the central budget. According to Decision no. 7/2020. (V. 13.) AB of the Constitutional Court, the Parliament violated Article VI (3) and Article 39 (2) of the Fundamental Law by omission. The deadline set by the Constitutional Court for remedying this situation has passed without any results.

3. With regard to banking secrets, in a constitutional complaint lodged against the decision of the Curia, the Constitutional Court ruled that access to dual-nature data - processed by Eximbank, falls under the concept of banking secret and is data of public interest or data accessible on public interest grounds - is not guaranteed at all in this regulatory environment. The restriction of public access is comprehensive, not tailored to what is strictly necessary and proportionate, and there is no possibility of discretion regarding the disclosure of data. The legislator violated the Fundamental Law by failing to establish guarantees that would allow for the enforcement of freedom of information in relation to the disclosure of banking secrets that

classify as data of public interest or data accessible on public interest grounds and are processed by Eximbank that performs public tasks and manages public funds. Act LXXVI of 2023 provided for an exemption from banking secrecy with regard to the identity of the customer and the amount of the transaction, but it did not allow for discretion with regard to other data, which, in the opinion of the speaker, also constitutes an unjustified restriction on freedom of information.

4. With regard to ministerial discretion, the Constitutional Court, in its ruling on a constitutional complaint lodged against the decision of the Curia, stated that the executive power also makes discretionary decisions in determining foreign affairs and foreign economic interests, but its activities are nevertheless subject to control: the political control of the success of foreign and foreign economic policy and the consequences thereof – whether the government remains in power or is replaced – are exercised by the voters in elections. In the proceedings initiated in this regard, the court may examine whether the case actually raises a (foreign) policy issue, whether the legal norm containing the exemption has been laid down in law, whether the statement issued in relation to the refusal originates from the competent (foreign affairs) minister, and whether its content classifies the disclosure of the requested data as contrary to the country's foreign policy interests. However, the dissenting opinion attached to the decision pointed out, in line with the speaker's position, that the current regulation could lead to the erosion of freedom of information and create an unjustified shift of power in the system of checks and balances based on the separation of powers.

5. With regard to trade secrets, both the Court of Appeal and the Curia have ruled that, in cases where the disclosure of data of public interest is refused on the grounds of trade secrets, it is necessary to provide clearly defined arguments and reasons that form the basis for a substantive examination. A general reference by the defendant without specific facts is not sufficient to justify the refusal and to carry out a balancing of interests. Following the public procurement procedure, the enforcement of the fundamental right to freedom of information cannot be restricted on the grounds of ensuring fair competition and equal opportunities. When invoking trade secrets, the holder of the secret is obliged to specify the data affected by the restriction and to provide appropriate reasons justifying the restriction of public access.

6. With regard to the right of access to documents, the legal provisions governing access to documents in administrative proceedings, and the provisions of procedural laws applicable to certain court proceedings restricting access to and copying of procedural documents constitute provisions restricting access to data of public interest and data accessible on public interest grounds, as defined in Section 27(2)(g) of the Info Act.

7. Previous court practice has also stated that, in relation to the issue of qualitatively new data, the requested body cannot be obliged to produce data that does not exist in the requested form if its creation would involve a disproportionate amount of effort, However, the obligation to disclose data of public interest does not require the controller to keep (process) the data of public interest to be disclosed in the requested form, i.e. compiled in a collection.

In its ruling on a constitutional complaint against a decision of the Budapest Court of Appeal, the Constitutional Court ruled that if the data request concerns the collection of existing and processed data, its selection according to specific criteria and, for example, its arrangement in a table, the request cannot, in principle, be refused. Restricting public access is constitutionally justified if it is justified by the enforcement of another fundamental right or the protection of a constitutional value, eg. ensuring the smooth functioning of public bodies and the performance of their tasks may be such a constitutional value. Subsequently, Infotv. was also amended in accordance with the relevant judicial and Constitutional Court practice, which is regulated in Section 30(2a) of the Infotv.

8. With regard to the conduct of the proceedings, the Curia ruled that it is not a means of promoting the success of the case, nor does it extend to the preliminary assessment of the

probative value of the evidence and the notification of the parties thereof. The court's duty to intervene does not mean that it should call on the party to present further facts that it has not referred to itself, nor does it have any obligation to inform the party if a statement is too general to lead to a successful outcome in the case. The Code of Civil Procedure merely provides an opportunity to eliminate minor deficiencies and contradictions in statements already made.
II. In the rest of the presentation, the speaker highlighted the relationship between personality rights and data protection, the differences between data protection lawsuits and personality rights lawsuits, the possible sanctions, and how compensation is applied. In the case of the Civil Code, the personal right to privacy [Civil Code 2:42 (2)], while in the case of the GDPR and the Infotv, the fundamental right to the protection of personal data [Charter Article 8 (1), Article 16(1) TFEU, Article VI (3) Fundamental Law] constitutes the right, the enforcement of which is guaranteed by substantive law. When enforcing a claim, the Civil Code, the GDPR and the Infotv. differ in terms of the legal object to be protected by law and the subjective right to which the person is entitled.
In connection with the data protection lawsuit, it referred to the European Court of Justice's decision in Case C-300/21, according to which the concepts of "damage" and "non-pecuniar damage" within the meaning of Article 82 of the GDPR must be given an independent and uniform definition as concepts specific to EU law. The rules on specific liability for damages are contained in Article 82 of the GDPR and Section 24 of the Infotv, depending on the law governing data processing. The latter applies to the processing of personal data for law enforcement, national security and defense purposes. Concluding his presentation, he also addressed the issue of multiple claims in relation to the difference between the claims that can be enforced with regards to the violation of the two subjective rights.

Péter Báldy, Deputy Director, ELTE Faculty of Law Institute for Postgraduate Legal Studies:

Data protection training in Hungary

Training in the field of data protection in Hungary began at the end of the 20th century, initially mainly in the form of corporate training and adult education. At the end of the first decade of the 2000s, the first higher education courses appeared that partially included data protection knowledge, and since 2010, specialized training courses have been launched that deal specifically with the protection of personal data. Today, six universities (the Faculty of Law and Political Sciences at Eötvös Loránd University, Gábor Dénes College, the Faculty of Law and Political Sciences at the University of Miskolc, the National University of Public Service, the Faculty of Law and Political Sciences at the University of Pécs, and the Faculty of Law and Political Sciences at the University of Szeged) offer nine specialised training programmes for students with and without a law degree. Approximately 1,600 students have graduated from these programmes, and since 2009, more than 1,000 students have graduated from the ELTE Faculty of Law's Institute for Postgraduate Legal Studies in specialised courses on data security and data protection.

Looking at the role of NAIH in these training courses, it can be said that the Authority is involved in almost all of them: the staff participates in the training courses as students or lecturers. In 80-90% of higher education courses in Hungary, students can listen to lectures and ask questions directly from NAIH personnel in leader positions. It can be said that the Authority supports professional training and learning.

As far as data protection knowledge is concerned, the practice, procedures and cases of the NAIH show that the knowledge and skills acquired in specialist legal training build on each other: A few years ago, it was still a daydream, but today it is increasingly becoming a reality that most data protection professionals and controllers are familiar with the basic concepts, data processing actors, basic principles, legal bases, and information obligations, i.e. Articles 1-14 of the GDPR. At the same time, it is clear that the finer points of exercising data subjects' rights and incident management are reserved for professionals with a higher level of knowledge. And although they affect many people, there are still only a few who know, understand and apply the rules of automated decision-making, impact assessment or international data transfers regulations as a skill. It is not possible to acquire these elements of knowledge during traditional one- or two-day corporate training courses, but even several months of further training are not sufficient to develop the appropriate skills. This is why the introduction of micro-certificate training in data protection is such an important initiative. Its aim is to enable participants to acquire specific knowledge and skills in the areas of impact assessment, information provision and balancing of interests.

***

Júlia Sziklay, Vice President of International Affairs, said at the close of the conference that 30 years ago, when, following a call from László Majtényi, the first data protection commissioner, she knocked on the door of the newly formed Data Protection Commissioner's Office on Tüköry Street, she began her work of protecting information rights in an environment very different from today's. It is unimaginable for young people today, but in the 1990s, the internet was just beginning to spread, there were hardly any mobile phones, etc. It is natural that the changes of the legal, political, and technical environment have also brought about institutional changes. She hopes that the institution will live to see its next anniversary, that in 30 years' time it will still be able to fulfill its constitutionally designated role, and that its employees will be, just as she is now, proud of their workplace. She thanked her colleagues for their help in organizing the conference, with special thanks for the dedicated work of Gabriella Dél, a member of the Cabinet of the President.

Budapest, 2025.