Bundesverwaltungsgericht

ACA-Europe Colloquium
ReNEUAL II – Administrative Law in the European Union
Administrative Information Management in the Digital Age

Leipzig, Germany

Answers to questionnaire: Hungary

Activity co-financed by the Justice Programme of the European Union

ANSWERS TO THE QUESTIONS REGARDING ACA-COLLOQUIUM RENEUAL II – ADMINISTRATIVE LAW IN THE EUROPEAN UNION ADMINISTRATIVE INFORMATION MANAGEMENT IN THE DIGITAL AGE, 11 MAY 202 BUNDESVERWALTUNGSGERICHT (FEDERAL ADMINISTRATIVE COURT), LEIPZIG

I. Shared databases, structured information mechanisms or duties to inform of national authorities and the case law of your court or other courts of your country

Background: Book VI establishes in Art. VI-2 (1)-(3) three categories of (advanced) inter-administrative information management not covered by the (more basic) rules for information exchange under the obligations of mutual assistance regulated in Book V (in order of their level of integration): structured information mechanism; duties to inform, and (shared) data-bases. They are defined in Art. VI-2 (see also Introduction to Book VI paras 17-23 and paras 5-8 of the explanations of Book VI).

1. Does your national legal order establish mechanisms of information exchange among authorities within your country which are similar to those categories as defined in Book VI? If so, please provide the most important examples from a range of legal domains, describe how they work and classify them into the categories as defined in Book VI as far as feasible.

Hungarian national legal order establishes some similar mechanisms of information exchange among authorities to those categories defined in Book VI.[1] as follows:
Act CL of 2016 on General Public Administration Procedures [Section 4] describes the principle of effectiveness: "the authority, in order to be effective, shall organize its activities so as to impose the least amount of expense upon all parties to the proceedings, and to close out the proceedings as fast as possible without prejudice to the requirements for ascertaining the relevant facts of the case, through ***the integration of advanced technologies***." This expression of the advanced technologies refers on the one hand to the IT system operated by the public authorities and on the other hand to the rules of the electronic transactions.

Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions covers matters related to electronic communication between cooperating bodies (this includes, inter alia, government bodies, local authorities, other legal entities vested with administrative competence by an act or government decree, courts, etc.) and determines rules regarding the exchange of information. From these legal norms we should highlight the following regulations: if the cooperating body is aware that any information which it does not possess but which is necessary for a matter before it or for carrying out its duties, and - in case of personal data or classified information - which the cooperating body is authorized by law to retain, is available from a ***primary source of information***, it shall obtain such data or information from the primary source of information, provided that it is not excluded by law. The information shall be considered available from a primary source of information: if listed in a public register; if not listed in a public register but originates from a cooperating body; or if so provided for by

[1] Hungarian legal scholars examined Book VI. in detail. See: HAJAS Barnabás - KOI Gyula - GERENCSÉR Szabolcs Balázs - BERKES Lilla - BENCSIK András - HULKÓ Gábor - FEHÉR Júlia - LAPSÁNSZKY András - POLGÁR Miklós: VI. könyv – Információáramlás, *Pro Publico Bono - Magyar közigazgatás,* 2017. 2. klnsz., 196-241.

legislation with the primary source of information indicated. [Section 60 of Act CCXXII of 2015].
If the information which the cooperating body does not possess but which is necessary for a matter before it or for carrying out its duties, and - in case of personal data or classified information - which the cooperating body is authorized by law to retain cannot be obtained from a primary source of information but the cooperating body is aware of the fact that it is available from a ***secondary source of information***, it shall obtain such data or information from the secondary source of information by way of electronic means. The information shall be considered available from a secondary source of information: if it was obtained by a cooperating body from a primary source of information; or if it originates from a body other than a cooperating body and was obtained by a cooperating body from a non-cooperating body. [Section 61 of Act CCXXII of 2015].

The cooperating body defines its' ***information exchange protocol*** and in this protocol it specifies the type of information available as primary and secondary source of information, and the bodies having access to the information; the particulars of the cooperating body's platform for the disclosure of information by automated process, and the type of information that can be transmitted through the platform for the disclosure of information and the conditions of disclosure; the conditions for the disclosure of information by way of electronic transaction. By the request for exchange of information the cooperating body shall accept the conditions laid down in the published information exchange protocol and shall undertake to be bound by them. [Specified in section 65 of Act CCXXII of 2015].

The cooperating bodies shall transmit information electronically by way of ***simple information exchange***, or by way of ***disclosure by automated process***. Disclosure of information by automated process means the disclosure of information by a cooperating body without human intervention. Simple information exchange is exchange of information between cooperating bodies other than the disclosure of information by automated process.

We should also note that ***there is no common regulation for all public registers*** (common databases) with common rules guaranteeing the management of those registers in general. We should also underline that some Hungarian public registers (common databases) are part of the ***national wealth***, which enjoys enhanced protection regulated by an Act, detailed in a Government Decree.[2]

Finally, we should emphasize that Act CL of 2016 on General Public Administration Procedures describes only rules that are related to ***official records and registers***. The authority shall keep the data specified by law in official records and registers if: making entries in records and registers, the amendment and deletion thereof creates, changes or terminates specific rights and obligations of clients, or the purpose of keeping such records and registers is to offer

[2] See: Act CXCVI of 2011, Act CLVII of 2010 and Government Decree 38/2011(III. 22)

authentic proof or confirmation of data therein contained. This a register is called official public register.
There is no uniform, common regulation on the cooperation between Hungarian official registers and public registers. Thus, the data contained in ***sectoral public registers*** is only partially used. The lack of common rules is a consequence of the fact that public registers are created by sectoral (administrative) legislation and, secondly, the normative background of the various registers can be found at different levels. Finally, we should note that legal and IT developments are certainly needed to make these registers more interoperable.

2. Are there additional mechanisms of information exchange among authorities within your country which are not covered by those categories? If so, please provide examples, describe how they work and explain their specifics in relation to the ReNEUAL categories.

Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions specifies the following forms of collaboration:

- ***cooperation in decision-making processes and making statements***
  In this case the cooperating body, if it knows that a decision of another cooperating body is required for a case before it or for carrying out its duties, and such decision can be adopted ex officio or in proceedings that can be initiated by the requested cooperating body, the requesting cooperating body shall send its request by way of electronic means to the body entitled to adopt the decision in question.
  [Specified in Section 70 of Act CCXXII of 2015]

- ***central storage of sound and/or video recordings, audio-visual recordings***
  The body designated in the Government decree (hereinafter referred to as hosting provider) shall operate a central repository to provide for the storage - via IT application - of sound and/or video recordings, audio-visual recordings made by the manager of public roads; by the police in the context of traffic control measures; by cameras installed by the police; by cameras installed by the local community patrol; by private security services to the extent required for the discharging of their duties relating to the protection of private property of providers of financial services, financial auxiliary services open to the general public; by the entity collecting toll charges under the Act on the Fees Charged for the Use of Tolled Motorways, Main Highways and Regular Highways Based on Distance Travel, etc.
  The activities of the hosting provider are limited to storing recordings and data in the central repository and to provide IT applications. It is not allowed to access the recordings and the data kept in the central repository and may not perform any other form of data processing operation with such recordings and data.
  If the police, the national security service, the professional disaster management body, and/or - in criminal proceedings - the court, the public prosecutor's office, the investigating authority and the body conducting preliminary proceedings is allowed to receive - as provided for by law - recordings and data made by a statutory user of central repository, the statutory user of the central repository shall - if it uses the central repository - provide for the data transfer through the hosting provider's IT application.

Meanwhile the hosting provider may not be requested to release recordings or data made by a statutory user of the central repository, transmission of data shall be carried out in accordance with the data transmission rules set out in the sectoral act.
[Specified in Section 73/A of Act CCXXII of 2015]

Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions also states that administratives bodies shall co-work if their registers contain address data. In order to facilitate the interoperability of the cooperating bodies' registers containing ***address data*** and to foster address management along uniform principles, a central address register shall be maintained. The central address register is an official list or record of address data designed to promote the interoperability of various registers, featuring information exchange services for addresses as a form of authentic data source for the benefit of registers maintained by cooperating bodies on address data. [Specified in Section 72 of Act CCXXII of 2015]

3. In your country, do there exist legal obligations or a political practice to conduct an impact assessment before such advanced forms of information exchange are established?

In Hungary, where a legal possibility for electronic transaction, exchange of information in this advanced form exists, there is ***no legal obligation or a political practice*** to conduct an impact assessment before such information exchange.

Before commencing the data processing operations, the data controller shall carry out an assessment of the impact of the envisaged processing operations on the exercise of the fundamental rights of the data subjects, by taking into account the prevailing circumstances, in particular its purpose, the categories of data subjects, and the technologies used in the course of the processing operation. If, based on the risk assessment carried out under this procedure, the envisaged data processing is likely to have a major impact on any fundamental right of the data subjects, the data controller shall, before commencing the data processing operation, prepare an assessment in writing of the impact of the envisaged processing operations on the fundamental rights of the data subjects ('***data protection impact assessment'***). [See: Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information Section 25/G].

4. Has your court (or other courts of your country) pronounced judgements on such mechanisms of advanced information exchange among authorities within your country? Are you aware of ongoing court proceedings concerning such matters? What are most important cases or principles established in this case law?

Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions entered into force on 1 January 2017. As the regulation is fairly recent, only a few cases have been delivered under this Act, and the adopted judgements are mostly related to electronic relations between clients and public authorities, and not to advanced information exchange mechanisms among authorities. Such a judgment is, for example, judgment no. Kfv. III. 37.971/2019/3, which states that a public administration decision shall contain the information that an appeal against it can also be filed in electronic form.

5.

a) Can a decision-making body in your country rely on information from partners of such national (!) information networks or is it obliged to scrutinize the information itself?

Background: In Case C-503/03 Commission v Kingdom of Spain [2006] the CJEU established an obligation for users of the Schengen Information System (SIS) to take advantage of the so-called SIRENE offices in the system in order to validate sensitive information provided through the SIS. This jurisprudence inspired Art. 25(2) SIS II-Regulation (EC) 1987/2006 and the general draft rule in Art. VI-21 of the ReNEUAL Model Rules.

Firstly, we note that if the cooperating body has any doubt as to the ***authenticity or existence of the information*** in its possession, it shall - save where excluded by legislation - obtain the information from a primary source of information by way of electronic means.

Secondly, if there is any doubt as to the applicability or authenticity of any information obtained from a primary or secondary source of information or contained in a document, the cooperating body shall notify the cooperating body known as the source of information thereof without delay, not later than the working day following the day of gaining knowledge, and that cooperating body shall open ***proceedings to review*** such allegation, and shall inform the cooperating body as to the results thereof. [See: Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions Section 60 (5); Section 63]

Finally, regarding ***official records and registers***, Act CL of 2016 on General Public Administration Procedures states that unless otherwise provided for by an Act, based on the authenticity of official registers, it shall be presumed - until proof to the contrary - that a party having acquired certain rights by relying upon data obtained from an official register was acting in good faith. Until proof to the contrary, data contained in official registers shall be presumed to be existent, and data deleted from official registers shall be presumed to be non-existent. Therefore, unless proven otherwise, the presumption is that the data recorded in the official records and registers are real.

b) If a decision-making body in your country is obliged to scrutinize information obtained from a national information network, what does this mean in practice? How far does this obligation reach?

If the decision-making body has requested the information, the cooperating authority dos not need to verify the data if the data is in a Hungarian public, official records.

6. In case of an information exchange between national authorities which concerns the transfer of personal data:

a) Does your national legal order provide for the automatic (i.e. without request) information of the person concerned?

Firstly, we emphasise that under Act CL of 2016 on General Public Administration Procedures (Section 27-28) the authority shall process the natural identification data for the identification of clients and other parties to the proceedings, personal data specified by the legislation governing the given case, and - unless otherwise provided for by law - other personal data considered essential for carrying out the proceedings effectively. The authority shall ***ensure that statutory secrets*** (hereinafter referred to as privileged information) are not disclosed to the public and cannot be obtained by unauthorized persons, and that all personal data are sufficiently protected. In its proceedings the authority shall process privileged information - subject to the provisions of other legislation in terms of procedure and scope - as it may be required in the course of its proceedings and/or which needs to be processed with a view to concluding the proceedings effectively. In justified cases the authority shall be entitled to order - upon request or of its own motion - that the natural identification data and home address of the client and other parties to the proceedings be handled confidentially, if such person could be exposed to extreme danger on account of his participation in the proceedings. The order shall be communicated to the requesting party.

Secondly, we note that Act CCXXII of 2015 on the General Rules for Trust Services and Electronic Transactions provides that in respect of personal data a cooperating body has in its possession for the administration of a matter in proceedings instituted upon the client's request or initiative, the cooperating body shall ***disclose such personal data*** to the body providing e-governance services, and that body shall process such personal data to the extent necessary for the administration of the said matter, on condition that the body providing e-governance services has informed the client of the material circumstances related to the data processing in accordance with the relevant regulations.

b) Does your national legal order provide for an enforceable right of the person concerned that he/she be informed of such an exchange upon request?

Yes, the cooperating body supplying personal data shall record its data processing operations carried out in respect of personal data disclosed under Act CCXXII of 2015 with facilities enabling the client to ***receive information electronically***, within not more than three days, if his data have been disclosed to a cooperating body, including the type of data disclosed, the name of the body, and the purpose and the time of disclosure.
[Section 53-54 of Act CCXXII of 2015]

7. Who is liable for any damage caused by malfunctioning of those national information networks or by false information entered into the system by a partner institution?

Background: In the legal framework of some European information systems the legislator established a substitutional liability or subrogation mechanism (Art. 48 SIS II-Regulation (EC) 1987/2006; see also Art. 116(2) Convention Implementing the Schengen Agreement; Art. 40(2), (3) CIS-Regulation 515/97). Art. VI-40 ReNEUAL Model Rules formulates a general rule along these lines in order to enhance the protection of individuals facing damages caused by such mechanisms. In addition, Art. VI-40(2) provides for a compensation mechanism among the participating authorities in order to provide incentives to comply with their respective legal obligations.

In advance we provide the information that the ***Supervisory Authority for Electronic Procedures*** is a body designated by the Government for facilitating and supervising electronic administrative procedures, for the cooperation and coordination of cooperating bodies, and tasked to carry out functions delegated in Act CCXXII of 2015 and the government decree implementing the Act. In its powers and responsibilities, the Authority shall maintain the registry of sources of information; accept notifications relating to information exchange protocols and information exchange agreements; maintain the list of data and document descriptions; adopt technical directives; and supervise the activities of cooperating bodies governed under the Act CCXXII of 2015, with the exception of overseeing and promoting the enforcement of the rights to the protection of personal data and to access to public information and information of public interest.
For the realisation of its last-mentioned powers, the Authority shall conduct supervisory inquiries to check the activities of cooperating bodies for compliance with the requirements set out in the Act and in its implementing decrees; shall conduct supervisory inquiries to check the information exchange protocols and agreements notified; may raise objection as regards the information exchange protocols it has received; shall examine the reports and recommendations submitted against cooperating bodies having regard to obligations provided for in the Act, on the basis of which it may make recommendations to the competent authority, or to the organ or person to lodge a legislative initiative; shall propose measures for cooperating bodies intended to uphold the provisions of this Act; shall draw up an annual inspection plan for regular and comprehensive supervisory inquiries. When requested by the Authority, cooperating bodies shall supply information that are necessary for keeping the registry of sources of information up-to-date. In case of failure to comply with the disclosure obligations, or if false information is supplied, the Authority shall launch a supervisory inquiry. Based upon the notification of information exchange protocols and information exchange agreements, and on the amendments thereof, the Authority shall open supervisory inquiry in monitoring the activities of the cooperating bodies for compliance with Act CCXXII of 2015 and its implementing decrees, including other related legislation, as well as the provisions of the information exchange protocols and information exchange agreements. The findings of the supervisory inquiry shall be summarised in a supervisory report. If the Authority obtains information in carrying out the supervisory inquiry that may present an information security risk, it shall immediately inform the authority responsible to oversee the security of the electronic information systems.

[Specified in Section 74-75 of Act CCXXII of 2015]
In case of personal data, if the ***data controller and/or the data processor*** acting on the controller's behalf or following the controller's instructions is in breach of a provision of a law or a binding piece of legislation of the European Union governing the processing of personal data and thus cause damage to others, they shall be liable for such damage. If the data controller and/or the data processor acting on the controller's behalf or following the controller's instructions is in breach of a provision of a law or a binding piece of legislation of the European Union governing the processing of personal data and thus, as a result, violates others' personality rights, the person whose personality rights are violated may demand indemnification from the data controller and/or the data processor acting on the controller's behalf or following the controller's instructions.
The data controller shall be exempt from liability for damages or for payment of indemnification if he proves that the damage was caused by or the violation of the personality rights is attributable to reasons beyond his control.
The data processor shall be exempt from liability for damages or for payment of indemnification if he can demonstrate that he has acted during the processing operations in compliance with all the obligations specifically applicable to data processors under the law or a binding piece of legislation of the European Union pertaining to the processing of personal data, and in due observance of the data controller's lawful instructions.
The data controller and/or the data processor acting on the controller's behalf or following the controller's instructions, and joint controllers or data processors acting on their behalf or following their instructions, in the event of non-compliance with obligations specifically directed to data processors by the law or a binding piece of legislation of the European Union pertaining to the processing of personal data,

- shall be jointly and severally liable for damage caused to the data subject, and
- shall be jointly and severally liable for payment of indemnification for any violation of the data subject's personality rights.

No compensation shall be awarded, and no indemnification can be demanded where the damage was caused by, or the violation of the personality rights is attributable to, intentional or negligent conduct by the person whose personality rights were violated. [See in Section 24. of Act CXII of 2011.]

8. In your national legal order, are there any specific safeguards or legal remedies of individuals considering information about them to be false or an exchange of information about them to be illegal? Is there a political or academic discussion about (further) needs for new or more specific legal safeguards in this context? Are there any recent legislative proposals on this topic?

Yes, in the Hungarian legal order ***specific safeguards*** and ***legal remedy possibilities*** are available for individuals in case false information has been provided about them or illegal exchange of information about them has occurred.

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information provides that regarding personal data processed by the data controller or the data

processor acting on the controller's behalf or following the controller's instructions, the data subject shall: have the right to be informed of the circumstances of data processing before the commencement of the processing ("***right to prior information***"); have the right to request the data controller to make available his personal data and information concerning the processing thereof ("***right of access***"); have the right to obtain from the controller rectification and/or amendment of his or her personal data upon request ("***right to rectification***"); have the right to obtain from the controller restriction of his or her personal data upon request ("***right to restriction of data processing***"); have the right to obtain from the controller erasure of his or her personal data upon request ("***right to erasure***").
In order to give effect to the right to rectification, if a piece of personal data processed by the data controller or a data processor acting on the controller's behalf or following the controller's instructions is inaccurate, erroneous or incomplete, the data controller shall rectify such data without delay, especially when so requested by the data subject, or – if it is compatible with the purpose of the processing – supplement them with additional personal data made available by the data subject, or by a statement made by the data subject in relation to the processed personal data.
This obligation shall not apply to the data controller if: accurate, correct and complete personal data are not available, and they are not supplied by the data subject either; or if genuineness of the personal data supplied by the data subject cannot be ascertained beyond any doubt.

We emphasize that the data subject (the individual) may bring an action before the ***court*** against the data controller or the data processor in relation to the processing operations falling within the data processor's scope of responsibilities if he is of the opinion that the data controller and/or the data processor acting on the controller's behalf or following the controller's instructions processes his personal data in breach of the provisions of the law or a binding piece of legislation of the European Union governing the processing of personal data. The burden of proof to ascertain that a given data processing has been in conformity with the provisions of the law or a binding piece of legislation of the European Union governing the processing of personal data lies with the data controller and/or the data processor. If the court rules in favour of the plaintiff, it shall establish the violation and shall order the data controller and/or the data processor: to terminate the unlawful processing operations; to restore the lawfulness of data processing, and/or to perform certain well-defined activities so as to ensure the exercise of the data subject's rights, and shall rule on any claim for damages or indemnification, where applicable. [Specified in Section 14-24 of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.]

The supreme judicial forum of Hungary, the ***Curia has also delivered several judgements*** related to these rights of the individuals. Recently the Curia has stated that data managed by the data controller and indirectly allowing for the identification of the person – through linking additional data not managed by the data controller – shall constitute personal data and shall remain such until their connection with the data subject (individual) can be restored. A data subject (individual) can be restored /qualified/, where the data controller has the technical conditions necessary for the restoration of the connection. [*BH2019. 272*]

Finally, we note that last year ***very vivid political and academic discussions*** took place in Hungary in relation to data protection. Due to EU regulation, several provisions of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information were amended in 2018.
Moreover, several books were published on data protection and electronic transmissions, e.g. PÉTERFALVI Attila - RÉVÉSZ Balázs - BUZÁS Péter: Magyarázat a GDPR-ról, Budapest Wolters Kluwer; 2018. *('An explanation of GDPR'),* GÖRÖG Márta - MENYHÁRD Attila - KOLTAY András: A személyiség és védelme az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül, Budapest Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar ; 2017. *('Personality and its protection – the enforcement of Article VI of the Fundamental Law of Hungary within the Hungarian legal system');* BARANYI Bertold - HOMOKI Péter - KOVÁCS A. Tamás: Magyarázat az elektronikus ügyintézésről, Budapest Wolters Kluwer; 2018 *('An explanation on electronic administration').*
Currently, there is also a legislative proposal promoting the ***simplification and electronisation of administrative proceedings.***

II. Cross-border and multi-level information sharing and the case law of your court or other courts of your country

1. Has your court (or other courts of your country) pronounced judgements on such EU mechanisms of advanced cross-border or multi-level information exchange among European authorities? Are you aware of ongoing court proceedings concerning such matters? What are most important cases or principles established in this case law?

Hungarian courts made several references to cross-border or multi-level information exchanges having taken place ***mostly between Hungary and another EU country*** (hence not between Hungary and an EU authority), and they constituted not so high-level information exchange as the ones discussed above.

A few court cases contain references to deeper, more organised cooperation between Hungarian and EU or EU member state authorities. We invoke, as an example, mutual assistance availed of for the enforcement of claims relating to taxes, duties and other measures (Kfv. III. 35.021/2016/5). In another instance of such reference, the court has stated that if an authority of another Member State has withdrawn a foreign national applicant's driving license, the issue by the Hungarian authority of a new driving license cannot be refused solely on account of the fact of withdrawal, the expiry of the withdrawal period must also be examined in all cases. After the expiry of the withdrawal period, compliance by the applicant with the eligibility criteria set forth for the issue of a new driving license in Hungary shall be examined under the relevant Hungarian rules (Kfv. IV. 37.779/2018/6). In another decision the Curia of Hungary, the supreme judicial forum of the country, has stated that the final report of the European Anti-Fraud Office (OLAF) constitutes admissible evidence for the recovery of agricultural and rural development aid, but does not exempt the Hungarian public authority from the obligation of

clarifying the facts, and the other party shall enjoy the guaranties enshrined in the Administrative Procedure Act (Kfv. IV. 35.698/2016/11).

2. Has your court (or other courts of your country) delivered judgements drawing on the CJEU case law in Case C-503/03 Commission v Kingdom of Spain [2006] or on Art. 25(2) SIS II-Regulation (EC) 1987/2006?
Background: see Question I.5.

No direct reference to the judgement adopted by the CJEU in case no. C-503/03 *(Commission v Kingdom of Spain [2006])* can be found in the judgements of the Hungarian courts. As to SIS II-Regulation (EC) 1987/2006, Hungary accepted Act CLXXXI of 2012 on the exchange of information within the second-generation Schengen Information System. Hungarian courts have delivered ***several judgements referring to the SIS II-Regulation***, for example, judgment no. Kfv. II. 37.730/2017/5; cases ***similar*** to case no. C-503/03 (*Commission v Kingdom of Spain* [2006]) can be found among Hungarian cases, namely case no. Kfv. III. 37.159/2017/8 and, as an even more pregnant example, case no. Kfv.VI.37.656/2018/9.
In case no. ***Kfv.VI.37.656/2018/9*** the applicant, a Moroccan national, travelled to Hungary illegally in 2015 and on 1 June 2015 applied for a residence card on the basis of his marriage to a Hungarian national. The first instance authority rejected his application and obliged him to leave Hungary until the last day of the third month following the date on which the first instance authority's decision became final. The first instance decision was upheld and supplemented by a statement of reasons by the decision of the second instance authority having acted on the applicant 's appeal. The Administrative and Labor Court dismissed the applicant's action filed against the final administrative decision. The Court stated that the applicant's marriage was not proven, therefore the refusal of the residence card was lawful. Despite the final, legally binding decision the applicant failed to leave the territory of Hungary and on 11 November 2016 he again applied for a residence card, based on his marriage. In its decision of 20 January 2017 the first instance authority repeatedly refused his application and ordered him to leave the territory of Hungary until the last day of the third month following the date on which the authority's decision became final. The authority stated that if the applicant failed to comply with the above obligation, the authority could order his expulsion. The authority also pointed out that there was a SIS alert from Austria with the applicant's personal data, according to which the applicant had been refused to access the Schengen Area on 12 November 2014 until 11 November 2017. The reason for issuing the alert was a final conviction for drug trafficking and assault. The authority stated that no cohabitation existed between the applicant and his spouse, and suspected that the marriage might have been concluded only to avoid expulsion. The Hungarian Police Authority also provided the information to the first instance authority that the applicant's presence posed a real, immediate and serious threat to Hungary's public security. The applicant filed an appeal against the decision. The appeal was accompanied by a document issued by the International Law Enforcement Cooperation Center on 21 February 2019, according to which the applicant was not included in the Schengen Information System at the time of the issuance of the document, and no alert had been issued in respect of him. Finally, the case was dealt with by the supreme court, the Curia of Hungary, which stated that the first instance court's judgment

was to be upheld because – among other reasons – the authority considered all circumstances and could not disregard the statements received from the Hungarian Police Authority. The court also took into account the fact that the applicant had illegally arrived in Hungary in 2015 and despite the refusal of his application for residence card and the order to leave the country, he had failed to leave Hungary and had applied again for a residence card. The court underlined that on 12 November 2014 another EU Member State – Austria – had refused the applicant's entry into the Schengen Area until 11 November 2017. The court also stated that the applicant did not prove that he had married and lived together with his wife from whom his child had been born. Based on the above facts the Curia of Hungary upheld the first instance court's judgment, finding that the applicant failed to meet several criteria to be met for exercising the right of residence and that his stay in Hungary constituted a direct and serious threat to public safety.

Finally, we note that due to the recent geopolitical situation, in the past years ***more and more cases*** related to third country nationals having spouses in EU member states, the right of entry and residence, and restrictions imposed on ground of public policy have been dealt with by the Hungarian authorities.

3. Has your court (or other courts of your country) delivered judgements drawing on a substitutional liability or subrogation mechanism in accordance with Art. 48 SIS II-Regulation (EC) 1987/2006, Art. 116(2) Convention implementing the Schengen Agreement, Art. 40(2), (3) CIS-Regulation 515/97) or similar provisions of EU law?

Background: see Question I.7.

Under Article 48 SIS II Regulation (EC) 1987/2006, individuals can bring an action before the civil court. There are a few judgements which invoke the above-mentioned EU laws, but none refers to the Articles specified in the question. However, a few cases refer to SIS, for example a Curia of Hungary judgement (no. Pfv. IV. 20.389/2015/4) states that it shall give rise to a claim for compensation on account of damage caused by an administrative authority if the police fails to properly send the warrant or to adopt a decision terminating a seizure and therefore the person concerned cannot avail of his right to complain – if the person proves his ownership. In the case at issue a seizure was made in consequence of an Austrian alert in the SIS.

4. In your national legal order, are there any new or specific legal safeguards with regard to cross-border or multi-level information sharing? Is there a political or academic discussion about (further) needs for new or specific legal safeguards in this context? Are there any recent legislative proposals on this topic?

Background: At least in some sector-specific secondary EU law new approaches are developed in order to avoid either gaps of judicial oversight or to minimize factual burdens for concerned citizens to initiate effective judicial review. One of these new instruments allows for trans-national representative legal action (compare Art. 111(1) Convention Implementing the Schengen Agreement; Art. 36 (5) CIS-Regulation 515/97).

In the field of administrative law, GDPR and e-privacy regulation have been vividly discussed in the past months in Hungary. At some conferences (e.g. at the 24-25 May 2017 Conference on ReNEUAL Model rules on EU administrative procedure in connection with Book VI. of the ReNEUAL Model rules) specific legal safeguards related to cross-border or multi-level information sharing were discussed, but currently no regulation exists on this topic.