Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Austria

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

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

11 May 2020

Bundesverwaltungsgericht (Federal Administrative Court), Leipzig

Questionnaire

Introduction:

National legal orders and European Union law are in many fields closely linked. Both underlie mutual influences. The jurisdiction of the European Court of Justice is not only relevant and binding as the interpretation and application of European Union law is concerned. Also, its jurisdiction partly affects the interpretation and application of national law. This phenomenon can be observed e.g. in the law of administrative procedure or of administrative court procedure.

On the other hand, European Union law is founded on the national jurisdictions of the member states. From an optimistic point of view it ought to be an essence of the best the national legal orders have to offer. In this line of thinking the European Court of Justice considers the national legal orders as source of inspiration in determining the general principles of European Union law which traditionally, i.e. before the Charter of Fundamental Rights came into force, were the sole source of fundamental rights within the jurisdiction of the European Court of Justice (cf. ECJ Case 4/73 (Nold), ECLI:EU:C:1974:51, p.507-508). Accordingly, the European Court of Justice has deducted many procedural rights in administrative procedure from the national legal orders. It is in the interest of the member states that the relationship between European Union law and the national legal orders remains one of mutual interchange, better: a dialectic process.

This is especially the case in evolving new legal fields like the law of composite and interlinked information management between various national authorities as well as between national and European Union administrative bodies. Such inter-administrative information management is a major component of administrative procedures implementing European Union law. It reflects the need of public authorities for reliable and up-to-date information from various sources in cases concerning cross-border public or private activities within the internal market. In order to provide such information the European Union has established sets of mechanisms for cross-border and/or multi-level exchange of information. Prominent examples are rapid alert systems providing information about risks for consumers caused by dangerous food or feed or other products, the Internal Market Information System (IMI), information systems in the field of customs and taxation, and the growing number of information

systems concerning migrants or travellers (Schengen Information System, Visa Information System, Eurodac). More recently, discussions arise that these systems may evolve into semi- or even fully automated decision-making systems.

This integration of various databases and other sources of information raises a number of legal questions: Can a decision-making body rely on information from partners of the information network or are they obliged to scrutinize them themselves? Who is liable for any damage caused by malfunctioning of those systems or by false information entered into the system by a partner institution? Is there a need for new legal safeguards of effective legal protection?

The ReNEUAL Model Rules on European Union Administrative Procedure contain in Book VI draft rules on inter-administrative information management which concern types of information exchange beyond the basic rules of mutual assistance covered by Book V of the Model Rules. The rules of Book VI shall inform the discussions at the 2020 colloquium in Leipzig in a similar way as the draft model rules of Book III concerning single case decision-making stimulated the seminar in Cologne at the end of 2018. In addition, the colloquium is supposed to recall the discussion within ACA concerning digital technology and the law with a stronger view on the decision making at the colloquium in The Hague on 14 May 2018.

The ReNEUAL draft is a project which has mostly been promoted by European scholars with expertise in European Union law, in various national legal orders as well as in comparative legal studies (http://www.reneual.eu/index.php/projects-and-publications/reneual-1-0). Yet, several legal practitioners, i.a. judges from several member states, have also contributed. The ReNEUAL draft is available in English, French, German, Italian, Polish, Romanian and Spanish. For the purpose of this questionnaire, Book VI (Administrative Information Management) is attached as a file in English. You will find links to other language versions on the ReNEUAL-website: http://www.reneual.eu/index.php/projects-and-publications/.

In contrast to the 2018 Cologne seminar, we will not discuss a resolution adopted by the European Parliament in 2016 on a proposal for a regulation for an open, efficient and independent European Union administration (EP-No. B8-0685/2016 / P8_TA-PROV(2016)0279). This draft focusses for good political reasons on single case decision-making and does not cover the topic of the Leipzig colloquium.

The colloquium 2020 to be held in Leipzig aims at further investigating into the national legal orders in order to assess their principles more profoundly and on a wider scale. ReNEUAL is very much aware of the fact that Book VI contains the most innovative part of the Model Rules. In addition, Book VI covers a highly dynamic field of law. Thus, Book VI itself will certainly evolve during the next years and ReNEUAL has already set up a new working group in order to update the existing rules and to investigate the need and the options for additional rules, especially concerning automated decision-making and the use of artificial intelligence in administrative procedures.

In line with this, the purpose of the Leipzig colloquium is to achieve a better understanding of the existing (additional) approaches of the national legal orders, to discover similarities and/or differences in order to promote the dialectic process mentioned above and thus both contribute to a better understanding of the principles of the European Union legal order derived from the essence of the member states' legal orders and enable a mutual learning process as well between national legal orders among themselves as between the national legal orders and the European Union's legal order.

Wherever you consider it appropriate, it would be helpful if you not only described your national legal order, but also compared your national legal order with the relevant provisions of Book VI of the ReNEUAL Model Rules. For this purpose the questionnaire makes reference to single provisions of Book VI in order to facilitate the links.

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) databases. 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.

To provide a better understanding of the situation in Austria we have chosen to discuss structured information systems similar to those described in Art. VI-2 (1) after databases in the sense of Art. VI-2 (3).

Several legal provisions foresee information duties for authorities as described in Art. VI-2 (2). A few examples are:

Pursuant to section 5 (3) of the Environmental Impact Assessment Act 2000 (Umweltverträglichkeitsprüfungsgesetz 2000 – UVP-G 2000) the authority (competent to conduct the EIA) shall communicate without delay the application, the relevant project documents and the environmental impact statement to the co-operating authorities for comments. The authorities

according to section 2 (1) subpara. 1 leg.cit. shall co-operate in the technical and legal assessment of the project to the extent required and shall submit proposals for the required subject fields and the respective experts. The aforementioned authorities are the authorities which, on the basis of administrative provisions, 1.) would be responsible for granting development consent or inspecting the project if the present federal act did not require the performance of an environmental impact assessment for the project, 2.) are responsible for inspecting the project or for issuing ordinances required for implementing the project (construction or operation) or 3.) have to be involved in the relevant procedures.

Several information duties exist pursuant to section 105 of the Aliens Police Act 2005 (Fremdenpolizeigesetz 2005 – FPG 2005). Security agencies have to notify the provincial police directorate if an alien is under suspicion of a criminal offence punishable by the ordinary courts and the underlying circumstances. If need be, the provincial police directorate then has to forward said information to another competent authority. Criminal courts have to notify the provincial police directorate if an alien is indicted on wilful charges, of legally binding sentences including a copy of the judgement or of the imposition and repeal of detention awaiting trial. Prisons (including court adjacent prisons) have to notify the provincial police directorate of the beginning and end of detention. Citizenship authorities have to notify the competent provincial police authority of the awarding of citizenship to an alien. Regional administrative authorities have to notify the competent provincial police directorate of applications for a change of name by an alien and civil courts have to notify of applications for adoption. Driving licence authorities have to notify of the issuance of a driving licence to an alien.

Further information obligations arise from sections 3 and 31 of the Federal Act on the General Rules for Procedures at the Federal Office for Immigration and Asylum (short: BFA-VG). These include that security agencies shall transmit to the Federal Office for Immigration and Asylum the identification data of aliens, which they have compiled and of which the Federal Office for Immigration and Asylum has already compiled differing identification data. Security agencies also have to notify the Federal Office for Immigration and Asylum of the suspicion of a criminal offence by an alien punishable by the ordinary courts and the underlying circumstances. Citizenship authorities have to notify the Federal Office for Immigration and Asylum of the awarding of citizenship to an alien as well as the forfeiture of citizenship. Personal statute authorities have to notify the Federal Office for Immigration and Asylum of marriages or registered partnerships of third country nationals (except marriages/partnerships to EU-citizens exercising their right to free movement). Regional administrative authorities have to notify the Federal Office for Immigration and Asylum of applications for a change of name

by an alien and civil courts have to notify of applications for adoption. Driving licence authorities have to notify of the issuance of a driving licence to an alien.

Pursuant to section 12 (2) Anti-Wage and Social Dumping Act (Lohn- und Sozialdumping-Bekämpfungsgesetz – LSDB-G) tax authorities have to transmit the results of their investigations concerning wage control to the competence centre for anti-wage and social dumping. If requested by aforementioned competence centre tax authorities have to conduct further precisely described measures in addition to previously transmitted investigation results.

Section 46 of the Austrian Trade Act (Gewerbeordnung – GewO) foresees that the holder of a trade licence can - if not stipulated otherwise - exercise his business licence in additional business units after notifying the competent authority. This obligation to notify includes notification about opening/closing of additional locations and the relocation of a main business or an additional business unit. The competent authority then in turn has to notify the authority competent for the location of the new/additional businesses (if a different authority would be competent).

In Austria we have several databases in the sense of Art. VI-2 (3), therefore only a few are mentioned here:

The first structured information mechanism to be mentioned is the Central Residence Register, in which every resident in Austria is registered with their principal residence and - if existing - a secondary residence. In this register the identity data (name, sex, date of birth, central register number, citizenship, etc.) and the residence data are recorded. The Central Residence Register is instituted at the Federal Ministry for the Interior. Registrations are being handled through the registry offices (Meldebehörde, Standesämter) and the citizenship offices of the cities and municipalities in Austria. All administrative authorities (eg. district authorities, police authorities, administrative courts) can access this database online. Upon application, public notaries, banks, lawyers, insurance companies, etc., who were vetted by the ministry, can obtain direct access to this system.

The Driving License Register is a database, which is instituted at the Federal Ministry for Transport, Innovation and Technology. It contains personal information of people holding driver’s licenses, expert witnesses (including doctors), driving schools, public health officers and traffic psychologists. It is used to gather the necessary data for granting driver’s licenses, conducting traffic controls as well as a record of certain driving offences. It can be accessed by district authorities and police.

The Identity Documents Register is a public registry instituted at the Vienna Federal Police Headquarters and contains information about issued passports, bans on passports, change of information on passports as well as information if an identity card was issued. It can be accessed by municipal authorities (concerning elections and voting cards), passport authorities and police.

The Register of Enterprises is instituted at the Statistics Austria. Statistics Austria is the Austrian Central Statistics Office, which is a federal institution under public law. This register is kept to store information (inter alia) about identification characteristics of the enterprises (e.g. designation, name, legal form, commencement and conclusion of business activity and commercial register number or central register of associations number, register of trade number, serial number in the supplementary register for other data subjects), address characteristics, ÖNACE code for main activities, in the case of legal entities, partnerships, associations and societies, the persons entitled to representation according to their constitution, codes in the official processes for the unambiguous identification of units of the register of enterprises (e.g. tax number, VAT number, data processing register number) and the register of enterprises code that shall be assigned by Statistics Austria at the time the enterprise is first entered. Statistics Austria grants the institutions of the Federal Government, the federal provinces, municipalities, social insurance institutions and statutory interest groups and in particular the institution of the Federal Government that is responsible for the operation of the Corporate Service Portal for the purposes of e-government online access to the data of the register of enterprises, insofar as this is required for the performance of their statutorily conferred duties and serves economic administrative purposes. Online access is free of charge with the exception of the implementation costs incurred by Statistics Austria for establishment of this access. The provisions of the Statistics Act concerning the register of enterprises also stipulate several duties to inform other authorities (in the sense of VI-2 (2)), which are necessary to obtain the information stored in the database.

Several additional databases exist, which cannot only be accessed by every authority but also by the general public (with restrictions applying to the freely accessible data).

The Central Register of Associations contains information about the legal status of associations, who is authorized to represent them, information about said authorized people, the asssociation’s name and their competent authority, the Central Register of Associations number, the date when it was formed, seat and mailing address as well as (if existent) a ban of disclosure of information to the public. Access to the Central Register of Associations is available online to the public, with several reservations. The data, which can be accessed

freely by everyone, only includes information about the Association's name and the people authorized to represent the association unless there is a ban of disclosure. The Central Register of Associations is instituted at the Federal Ministry for Interior, which (upon application) can grant remote access to the register in a way that enables public bodies to fulfil their legal obligations.

The Austrian Business Licence Information System is a publicly available database, which includes the name of the business license holder, the competent authority, the Business Licence Information System number, date of issuance of the business license, the business location, the name of the trade, the designation of trade (including a description) as well as the managing director under trade law. It is instituted at the Federal Ministry for Digital and Economic Affairs.

The Commercial Register contains information on all registered Austrian businesses (see Section 2 of the Commercial Register Act [Firmenbuchgesetz – FBG]). The documents on which those entries are based are stored in an electronic document archive kept by the Ministry of Justice. The company information and the document collection are available to the public online, but access is chargeable. Company data is also available to Austrian authorities through the portal of the Federal Computing Centre (BRZ).

The Austrian Land Register is a public register of all real estate properties and is maintained by the district courts. The register records ownership as well as rights pertaining to or charges upon real estate property. The Land Register consists of the main register ("Hauptbuch"), the collection of documents, the land register file ("Grundbuchsmappe"), the record of landowners and landed properties contain auxiliary information. In the main register, every landed property has its own entry (organised by entry numbers, "Einlagezahl", "EZ"), which consist of three folios: folio A ("A-Blatt", property particulars), folio B ("B-Blatt", property owner(s)), folio C ("C-Blatt (encumbrances on the property)). The collection of documents contains all the documents, which served as basis for the registration of a landed property. In recent years the Land Register has been
digitized and can be accessed online by authorities and the public requests, however, are not free. The respective billing centres can be accessed via website of the Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice. Furthermore extracts can be obtained at every district court and mapping office.

Concerning information systems similar to structured information mechanisms:
The criminal record register is a public register in which criminal convictions are registered. It is instituted at the Vienna Federal Police Headquarters. The criminal record certificate is a document containing either all of a person's registered convictions or the information that there are no such convictions. Information is only to be provided if requested to all national authorities, Federal Police departments and (concerning military personnel) to military commanding officers, authorities of other EU Member States (under certain limitations) and youth welfare authorities to avoid or avert an imminent threat to a minor through a specific person.

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.

All bodies of the Federation, the provinces, the municipalities and the municipality associations as well as the other self-administering entities are, within the framework of their legal sphere of competence, under the obligation of mutual assistance (Article 22 of the Federal Constitution, Bundes-Verfassungsgesetz – B-VG).

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?

There is no specific assessment procedure for advanced forms of information exchange. However, as of 2013 laws and regulations as well as major projects (eg. procurement activities, infrastructure projects) have to undergo an assessment of their effects and will be discussed on basis of their desired outcomes and outputs. Through the definition of indicators the output is measureable. Regulatory Impact Assessment is the implementation of the principle of outcome orientation into the policy-making and evaluation process. The assessed impact dimensions are financial impacts, impacts on the overall economy, impacts on businesses, environmental impacts, impacts in the field of consumer protection policy, impacts on administrative costs for citizens and enterprises, social impacts, impacts on children and young people and impacts regarding equality of women and men. After five years (at the latest) the previously defined indicators and milestones for the defined objectives and expected impacts are compared to the actual situation and in addition the existence of any further impacts is evaluated.

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?

There are many decisions concerning specific aspects of the individual registers or information exchange systems, but none that address information exchange systems as such.

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?

Pursuant to section 47 of the General Administrative Procedure Act 1991 (Allgemeines Verwaltungsverfahrensgesetz 1991 – AVG) the veracity of public deeds and private deeds is to be judged by the authority in accordance with sections 292 to 294, 296, 310 and 311 of the Code of Civil Procedure (Zivilprozessordnung – ZPO). In this connection, however, section 292 para. 1 first sentence of the Code of Civil Procedure shall apply only to the extent that public deeds issued by domestic authorities shall furnish evidence also on such facts and situations of law, which constituted the basis for their issuance and are expressly named in the deed.

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?

Generally speaking a public deed has presumption of full veracity of what is established in said deed. A public deed is a deed, which was produced in the foreseen manner by an Austrian, national authority within its competences (regardless of the way it was accessed, as for instance via an information network or register). This presumption, however, can be refuted if reasons for incorrectness are given and evidence is produced, which is deemed sufficient to refute this statutory presumption of full veracity (Supreme Administrative Court judgement from 18.11.2013, 2013/07/0165; available in German: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vwgh&Dokumentnummer=JWT_2013070165_20131118X00). If reasonable doubt about the veracity of the deed arise the authority has to conduct an ex officio investigation.

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?

No.

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

Art. 15 General Data Protection Regulation (GDPR) establishes the general right of the data subject to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Federal Act concerning the Protection of Personal Data (Datenschutzgesetz - DSG) contains special provisions concerning the processing of personal data for the purposes of security police, including the protection of public security by the police, the protection of military facilities by the armed forces, the resolution and prosecution of criminal offences, the enforcement of sentences and precautionary measures involving the deprivation of liberty.

In section 44 of the Act concerning the Protection of Personal Data it is stipulated that every data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed and where that is the case, access to the personal data and the following information:

1. the purposes of and legal basis for the processing,
2. the categories of personal data concerned,
3. the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations,

4. if possible, the period for which the personal data are planned to be stored, or if that is not possible, the criteria used to determine that period,
5. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject,
6. the right to lodge a complaint with the Data Protection Authority and the contact details of the Data Protection Authority, and
7. communication of the personal data undergoing processing and of any available information as to their origin.

In case access is not granted, the controller shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted in case the provision thereof would undermine a purpose under section 43 para. 4. These purposes are to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, in particular by obstructing inquiries investigations or proceedings of authorities or courts, to protect public security, to protect national security, to protect the constitutional institutions of the Republic of Austria, to enable the protection of military facilities by the armed forces, or to protect the rights and freedoms of others. The controller shall inform the data subject of the possibility to lodge a complaint with the Data Protection Authority. The controller shall document the reasons for the decision not to grant access. That information shall be made available to the Data Protection Authority.

However, there is no possibility to request such notifications in advance.

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?

The Federation, the provinces, municipalities, other bodies of public law and the institutions of social insurance – hereinafter named legal entities – are liable under the provisions of Civil Law for any damage to any person or any property caused by unlawful acts of persons at fault when enforcing the law on behalf of such legal entities; such persons implementing the law are not liable vis a vis the persons injured. Indemnity shall be paid only in terms of money (section 1 of the Liability of Public Bodies Act, Amtshaftungsgesetz – AHG). Therefore, if any damage is caused by malfunctioning or false information exchange systems damages can be claimed with the legal entity (in case of the abovementioned databases this would be the Federation) responsible for the damage. Damages are not due in case the injured person would have been able to avoid the damage by any legal remedy or by a complaint to an administrative court and a final appeal to the Supreme Administrative Court. No claim for any

indemnity can be based on any ruling of the Constitutional Court, the Supreme Court and the Supreme Administrative Court.

Furthermore, there is the right to compensation and liability as defined in Art. 82 of the GDPR.

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.

8. In you 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?

Pursuant to section 24 of the Act concerning the Protection of Personal Data every data subject has the right to lodge a complaint with the Data Protection Authority if the data subject is of the opinion that the processing of the personal data by an administrative body concerning the data subject infringes the GDPR, section 1 or Chapter 1, Article 2 of the Act concerning the Protection of Personal Data.

Said complaint has to include a description of the right considered to have been infringed, (to the extent it is reasonable) the description of the legal entity or the executive body or officer who is deemed to be responsible (respondent of the complaint), the facts from which the infringement is derived, the reasons for unlawfulness, the request to rule that the alleged infringement has been committed and the details necessary in order to decide whether the complaint has been lodged in due time. A complaint must be accompanied by the request on which it is based and the answer of the respondent to the complaint, if any. In the case of a complaint, the Data Protection Authority shall provide further assistance on request of the data subject. The right to have a complaint dealt with on the merits expires if the intervening party does not lodge the complaint within a year after having gained knowledge of the inci-

dent that gave rise to the complaint, but no later than within three years after the incident allegedly occurred. Late complaints shall be rejected. To the extent the complaint is shown to be justified, it is to be granted. If an infringement can be attributed to a private-sector controller, the controller shall be instructed to comply with the complainant's requests for information, rectification, erasure, restriction or data communication to the extent required to eliminate the infringement that has been found to exist. To the extent that the complaint is not found to be justified, it shall be rejected.

Pursuant to section 62 of the Act concerning the Protection of Personal Data, unless the offence meets the elements of Article 83 of the GDPR or is subject to a more severe punishment according to other administrative penal provisions, an administrative offence punishable by a fine of up to € 50.000 is committed by anyone who 1. intentionally and illegally gains access to data processing or maintains an obviously illegal means of access; 2. transmits data intentionally in violation of the rules on confidentiality (section 6), in particular intentionally uses data entrusted to him or her according to section 7 or section 8 for other prohibited purposes; 3. by giving incorrect information intentionally obtains personal data according to section 10; 4. processes images contrary to the provisions of Chapter 1, Part 3; or 5. refuses inspection pursuant to section 22 para. 2. Attempts shall be punishable. The Data Protection Authority shall be the competent authority for these decisions.

Whoever, with the intention to illicitly enrich himself or a third person or to harm someone regarding that person's rights guaranteed according to section 1 para. 1, deliberately uses personal data that has been entrusted to or has become accessible to him solely because of his professional occupation, or that he has acquired illegally, for himself or makes such data available to another person or publishes such data despite the data subject's interest in confidentiality, which deserves protection, shall be punished by a court with imprisonment of up to one year or with a fine of up to € 720,--, unless the offence is subject to a more severe punishment pursuant to another provision.

However, it is not possible to impose fines on authorities and public bodies, including entities which are formed under civil or public law and fulfil statutorily conferred duties.

The Supreme Court of Austria (which has final jurisdiction in matters of criminal and civil law) has issued decisions opening up a second possibility of filing claims concerning rights granted by the GDPR (see OGH 23.5.2019, 6 Ob 91/19d; available in German: https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20190523_OGH0002_0060OB00091_19D0000_000/JJT_20190523_OGH0002_0060OB00091_19D0000_000.html). This offers the

data subject the option of filing a law suit in civil courts in addition to the administrative proceedings before the Data Protection Authority. Furthermore, there is always the possibility of claiming damages - if any arose - from the infringement of the rights granted by the GDPR/Act concerning the Protection of Personal Data.

For alleged infringements of the rights on data protection by the courts in judicial matters (ordinary courts, administrative courts, Supreme Administrative Court) there is no appeal to the Data Protection Authority (which is an administrative body) but specific remedies exist within the respective courts.

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?

ECRIS

The Supreme Court of Austria has issued decisions stating that a criminal court can rely on information included in extracts from ECRIS concerning criminal convictions in other Member States and does not have to obtain the original court files (see for instance OGH 15.9.2015, 14Os91/15m; available in German: https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20150915_OGH0002_0140OS00091_15M0000_000/JJT_20150915_OGH0002_0140OS00091_15M0000_000.html).

EURODAC

In the judgement from 18.10.2017, Ra 2017/19/0291, the Supreme Administrative Court found that in Art. 23 para. 2 Dublin III-Regulation the differentiation in deadline for the submission of a take back request is based on whether the request is based on data obtained from the Eurodac-System or if the take back request is based on other evidence. Undoubtedly Art. 24 para. 1 leg.cit. continues this concept, depending on whether the take back request is based on a hit from the Eurodac-System or on different evidence, the time limit for replying to a take back request is different. This is on account of expediting the procedures; especially because the determination of competence for the proceedings based on data from the Eurodac-System will - generally speaking - make time consuming investigations dispensable (available in German:

https://www.ris.bka.gv.at/Dokumente/Vwgh/JWT_2017190291_20171018L00/JWT_2017190291_20171018L00.html).

Furthermore, the Supreme Administrative Court found in the judgement from 24.3.2015, Ra 2015/21/0004, that if a request for take back, which was essentially based on the statement of the alien, is accepted by the requested state the doubts, which arise from contradictory data within the Eurodac-System are refuted. It cannot be assumed a state would accept an unfounded request for take back (available in German: https://www.ris.bka.gv.at/Dokumente/Vwgh/JWT_2015210004_20150324L00/JWT_2015210004_20150324L00.html).

SIS

Pursuant to section 11 para. 1 subpara. 2 of the Settlement and Residence Act (Niederlassungs- und Aufenthaltsgesetz - NAG) an absolute reason for refusal of a residence permit is a prohibition of entry from another EEA-Member State. According to the wording of the law this criteria is also met if the prohibition of entry is imposed solely based on national law and it is irrespective of registration in the SIS (see Supreme Administrative Court judgement from 11.2.2016, Ra 2016/22/0012; available in German: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vwgh&Dokumentnummer=JWT_2016220012_20160211L00)

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.

The case C-503/03 is mentioned in several judgements of the Supreme Administrative Court. However, the main question in aforementioned judgements was whether it would be possible to limit an entry ban to the issuing country due to the fact that the alien has relatives in another EU Member State. The Supreme Administrative Court expressed the opinion that such a limitation of the entry ban is not covered within the wording of the law, however the family ties are to be considered if the alien later applies for an entry visa into the Schengen area in accordance with C-503/03 (see for example judgements of the Supreme Administrative Court, both only available in German, from 24.10.2011, 2004/21/0289, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Vwgh&Dokumentnummer=jwt_2004210289_20060926x00;and more recently from 3.9.2015, Ra 2015/21/0054,

https://www.ris.bka.gv.at/Dokumente/Vwgh/JWT_2015210054_20150903L00/JWT_2015210054_20150903L00.html).

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.

No.

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?

There are specific provisions in the Act concerning the Protection of Personal Data concerning the transmission of data to third countries or international organisations for purposes of the security police, including the protection of public security by the police, the protection of military facilities by the armed forces, the resolution and prosecution of criminal offences, the enforcement of sentences and the enforcement of precautionary measures involving the deprivation of liberty.

Any transfer of personal data by the competent authority, which is already being processed or intended for processing after the transmission to a third country or international organisation, can only take place if certain conditions are met. The transfer has to be necessary for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the enforcement of criminal penalties, including the safeguarding against and the prevention of threats to public security, and for the purposes of national security, intelligence, and the protection of military facilities by the armed forces and the recipient of said information is a competent authority for the previously defined purposes. If the personal data that is to be transferred was made available from another EU Member State, said Member State has to give their authorisation prior to the transmission.

Furthermore, it is only possible if the European Commission has adopted an adequacy decision pursuant, in the absence of such a decision, appropriate safeguards have been provided or exist, or, in the absence of an adequacy decision and of appropriate safeguards, dero-

gations for specific situations apply. It has to be ensured that an onward transfer to another third country or international organisation is permitted only subject to prior authorisation by the competent authority that carried out the original transfer and after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or international organisation to which personal data are transferred.
The transfer of personal data to a third country or an international organisation shall be permitted where the European Commission has decided pursuant to Article 36 para. 3 of Directive (EU) 2016/680 by way of an implementing act that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer does not require any specific authorisation.

In the absence of such a decision transfer of personal data to a third country or an international organisation may take place where appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or the controller, following an assessment of the circumstances relevant for the transfer of personal data, concludes that appropriate safeguards exist with regard to the protection of personal data. These transfers shall be documented, and the documentation shall be made available to the Data Protection Authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.
If no adequacy in the previously mentioned sense can be determined a transfer of information is only possible to protect the vital interests of a person, to safeguard legitimate interests of the data subject, where the law so provides, for the prevention of an immediate and serious threat to the public security of an EU Member State or a third country. In these cases a transfer is only permitted if no fundamental rights and freedoms of the data subject are infringed and public interest does not contradict the transfer.

There is no substantial academic or political discussion in Austria on this topic at the moment and there are no recent legislative proposals.
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).