Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Germany

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 inter-linked 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.

In the German legal order, there are several mechanisms of information exchange that can be qualified according to the criteria of the categories of art. VI-2 of the ReNEUAL draft. The following examples are not exhaustive, but are supposed to illustrate the range of information exchanges in Germany.

a) In the field of industrial law, a central professional register is operated by the Federal Office of Justice. This register actually is not a register of all established industries, companies or commercial activities, but includes especially enforceable and final administrative and judicial decisions denying or withdrawing approvals for running such an establishment, prohibiting specific commercial activities (like handling explosives, giving professional education in general or specifically for minors, public transport) or administrative or judicial sanctions with a context to commercial activities (like tax offences in connection with a commercial activity or

convictions for offences for illegal employment or other specific criminal offences related to employment. The register including all established industries, companies or commercial activities is not centralised, but operated by administrations on a local level (determined by state law, usually the municipalities). Additionally, there are specific registers for specific commercial activities like security firms or insurance brokers.

The main purpose of the central professional register is to collect information that is needed in order to determine whether a certain person is apt for running an established industry, company or commercial activity and to provide this information to the respective competent local authority supervising the establishment.

All administrative authorities and courts have to inform the central professional register about decisions, ascertainments and facts that are to be entered in this register. In order to pursue the main purpose of this register, it gives information on request of authorities that have to prosecute specific (administrative) violations of industrial law or to decide on specific applications of industrial law (for commercial activities that need to be authorised or for handling explosives) or on possible prohibitions of specific commercial activities. Also, public prosecution services, courts and the criminal police can request information when they are prosecuting specific criminal violations in connection with commercial activities. Additionally, the competition authorities and the Central Office of Financial Transparency can request certain information from this register.

For both, the information of the register by the different authorities and the information upon request of authorities by the register there are prescribed forms, which also include fill-in-boxes for which specific codes are to be used like for the types of commercial activity, for nationalities or some standardised texts.

The information exchanges in the context of this register can be qualified as structured information mechanisms according to art. VI-2 par. 1 of the ReNEUAL draft.

b) In the field of inhabitants, population registers are operated basically by all municipalities on a local level. In these registers, certain data and facts to prove the correctness of the data, which is thoroughly regulated by law, on all inhabitants of the municipality are saved. This data includes names, former names, date and place of birth, sex, nationalities, addresses, marital status, data on legal representatives, on the spouse and on minor children as well as data concerning the issuance of ID-cards or passports and, in the case of foreigners, the ID number used in the Central Register of Aliens (see below, f). Additionally, data and facts to prove the correctness of the data on the right to vote, on certain tax circumstances (tax number, membership in a religious community of public law, marital status, including certain tax data of the spouse and of minor children, the own tax number, the fact that there are reasons to deny a passport or that a passport has been withdrawn or a comparable decision on an ID-card has been taken, the fact that a permit on weapons or explosives has been granted and, if the person is not the owner, the owner of the house/flat are saved.

In general, the population register gets the relevant data directly from the person concerned. Everyone is obliged to register when moving to a new place and to give all the relevant information. Additionally, the population register is entitled to use, for its purposes, data that has been received from other administrative authorities or that it learns otherwise.

The population register transmits specific data to other administrative authorities, partly on request, partly by an automatically generated release order and partly on a regular basis on its own. Nevertheless, the specific information that can be transmitted are enumerated in a differentiated way: The list of specific data that can be transmitted on request contains most of the data concerning the respective person the request is about (i.e. it especially does not contain data on spouses or children). The list of data that can be released automatically is much more restricted and contains basically names, sex, date and place of birth and the current address of the person the release order refers to. For the automatically generated release order, there is, besides the basic norms in the parliamentary law a regulation by the Federal Minister of Interior, which prescribes the technical requirements for this automatic release. As far as the regular transmission of data by the population register is concerned, a specific legal basis is required to include an administrative authority in the list of addressees. This can be done by federal or by state law. Currently, among the addressees are the Federal Tax Office, the pension insurance, the Federal Central Register and the Central Register of Aliens, the Federal Motor Transport Authority, the Federal Office of Administration, the Federal Office for Personnel Management of the Army and the religious communities of public law.

The information exchanges in the context of these registers can probably be qualified as database according to art. VI-2 par. 3 of the ReNEUAL draft, although it has to be kept in mind that it is not a central register. Thus, it is maybe better described as a set of decentralised databases, although it might have elements of a structured information mechanism according to art. VI-2 par 1 of the ReNEUAL draft.

c) In the field of traffic law, there are registers on driving licences, on the driver's fitness to drive and on vehicles. The lower district administrations operate local registers on driving licences and on vehicles registered in their territorial circumscription. Additionally, the Federal Motor Transport Authority operates a Central Register on Driving Licences, a Central Vehicle Register and a Register on the Fitness to Drive.

The Register on the Fitness to Drive is supposed to save data that is needed especially to determine whether a person is fit to drive a motor vehicle or whether a person is entitled to drive a vehicle, to prosecute violations of persons who repeatedly commit criminal or administrative violations related to road traffic. Therefore, it saves, amongst others, final decisions of the criminal courts about specific traffic related crimes and on the withdrawal of a driving licence or a ban of issuing one, final decisions on administrative sanctions for specific severe traffic violations (usually connected with a suspension of the driving licence), on final refusals to issue a driving licence or on the withdrawal of a driving licence. Courts, public prosecution

services and other administrative authorities inform the Federal Motor Transport Authority immediately about the relevant data that is to be saved or that leads to a change or a deletion of an entry. Under specific requirements, they can do so directly accessing the register by remote data transmission. Interestingly, if there are doubts about the identity of a person, data of the population register can be used here, too. On the other hand, the data saved in the Register on the Fitness to Drive can be transmitted especially to authorities responsible for prosecuting crimes or executing criminal punishments, prosecuting or executing administrative sanctions on grounds of the Road Traffic Act or the Act on Personnel in Road Traffic or for administrative measures on grounds of the Road Traffic Act, regulations based on this act or on grounds of other specifically mentioned statutes in the field of traffic and road transport as far as it is necessary for the specific purpose of the saved data. The receiving authority may use the data only for the purpose it has been transmitted for, or for other purposes, it also could have been transmitted for. For the transmission to authorities of other states, there is a more restrictive regulation which also provides for an exception, if the receiving state does not guarantee am adequate level of protection of data. The law expressly says that transmissions of data from the Register on the Fitness to Drive are only permitted upon request, as long as a specific law provides for a duty of the register to inform. The law expressly allocates the responsibility for the admissibility of a transmission to the transmitting authority, if the transmission isn't done upon request, which is the more general case. In these cases, the requiring authority is the responsible one and the register only has to scrutinize the request on whether it falls within the competence of the requiring authority. Only if there is a special reason to scrutinize the admissibility of the transmission, the register does so. If further requirements are fulfilled, the potential addresses of transmissions may be granted access to the data of the register by automatically generated release order. The receiving authorities must, amongst others, guarantee the fulfilments of technical and organisational measures as demanded by the GDPR, and the Federal Motor Transport Authority produces records of the automatic transmissions, which are randomly checked on whether the requirements of the transmissions and of the use of the data are fulfilled.

The information exchanges in the context of this register can probably be qualified as a database according to art. VI-2 par. 3 of the ReNEUAL draft, although, because of the limits in regard of the requests, it also has some elements of a structured information mechanism according to art. VI-2 of the ReNEUAL draft.

The vehicle registers' purpose is to provide the necessary data, especially for the registration and surveillance of vehicles, for ensuring the insurance protection in the framework of the obligatory insurance for motor vehicles, for taxing motor vehicles, but also for executing the law on old vehicles to identify the registered keeper of a vehicle or the vehicles owned by a specific person. For this purpose, it saves specific technical data on every vehicle registered in the country and personal data of every natural person, or comparable data of a legal person to whom or which a licencing number of a vehicle is assigned to. The local registers gather these data from the person applying for a licensing number of a vehicle. Additionally, the insurance companies can communicate the existence or non-existence of an insurance for a vehicle and

the technical inspection bodies have to inform about data on security checks on vehicles. The law provides for the transmission of the relevant data on vehicles to administrative or other public bodies to carry out the tasks the data is saved for in the registers, to prosecute criminal or administrative violations, to prevent dangers for the public security and order, for the intelligence service, for measures in regard of waste disposal, to determine tolls and some others. These data can also be transmitted to vehicle producers in regard to calling back defective vehicles, to insurance companies in regard to ensuring insurance coverage and to technical inspection bodies in regard to their activities. The data on registered keepers of vehicles is, except for identifying the registered keepers only permitted for the prosecution of criminal offences, to prevent a specific danger for public security, for the intelligence services, for taxation purposes and to fulfil specific legal duties to inform in the context of social welfare. It cannot be obtained in another way. A few further exceptions are provided for, e.g. in favour of the Federal Criminal Office with regard to persons searched by an arrest warrant. A regular exchange of data between the local and central registers is explicitly provided for by law, if they are dealing with the vehicle concerned. There is also a regular exchange among local registers, from the local registers to insurance companies, to the tax authorities and some others. For the most usual purposes of the registers concerning vehicles as well as for a list of other communications the law provides for transmissions from the Central Vehicle Register are especially to the local registers as well as police and intelligence services. These transmissions are generated automatically. For more specific purposes transmissions may also be directed to the final receivers, for example to the operator of the toll system. However, automatically generated release orders may only refer to a specific vehicle or a specifically registered owner of a vehicle. They always need a specific legal basis that guarantees that the requested data are necessary for the receiver, that the technical and organisational requirements of the GDPR are fulfilled, and that the Federal Motor Transport Authority produces records of the automatic transmissions. The fulfilment of these requirements are randomly checked by the competent authorities. For transmissions to other states, the potential purposes of the transmissions are more limited. The other state must guarantee a comparable level of data protection. For the enforcement of damages, also individuals can obtain data from the registers, especially those about the identity of a registered keeper and about the insurance of a vehicle, if the individual indicates the registration number of a vehicle.

The information exchanges in the context of these registers can be qualified as a database according to art. VI-2 par. 3 of the ReNEUAL draft, although it is actually an interlinked system of the central and the local registers.

The registers on driving licences save data on the issued driving licences, locally or nationwide. The data especially contains names, date and place of birth of the person who has been issued a driving licence as well as the relevant data of the driving licence, like its class, validity, content and other details. The local registers may additionally save the address and nationality of the person as well as prohibitions to drive a vehicle or specific decisions on the driving licence, like withdrawals. The local driving licence authorities inform the Federal Motor Transport Authority immediately about any data to be saved, corrected or deleted in the Central Register on Driving

Licences. The data may be transmitted to public bodies that are responsible for the prosecution of criminal offences, for the execution of criminal sanctions, for the prosecution and execution of administrative sanctions on the grounds of the Road Traffic Act or for administrative measures on grounds of this act as far as driving licences are concerned. If the technical and organisational requirements of the GDPR are fulfilled, and the Federal Motor Transport Authority or the local registers produce records of the automatic transmissions in order to enable checks of the admissibility of the transmissions, transmissions by automatically generated release order are possible. Also here, specific rules for transmissions, including by automatically generated release order, apply for other countries. Individuals have the right to be informed upon their application about the data saved concerning their person.

The information exchanges in the context of these registers can be qualified as a database according to art. VI-2 par. 3 of the ReNEUAL draft, although it is actually an interlinked system of the central and the local registers.

d) In the field of social law, there are several specific regulations concerning social data, which complement the regulations of the GDPR. Public authorities which are involved in the granting of social benefits are entitled to use the social data they need for the duties assigned to them in the social law context. Yet, even within one single authority (e.g. a municipality), the social data of an individual has to be kept separate from any other activities of this public authority. Only in specific contexts, specific social data may be transmitted to other authorities. This applies for example to transmissions to the police, to public prosecution services and to courts, to which general social data, like name, data and place of birth, residence and name and address of the current employer may be transmitted. For these transmissions, a specific request referring to an individual case is always necessary. Moreover, the transmission is undue if the requiring authority can obtain the data in another way. For activities of other public bodies under social law, the rules for transmissions are less strict. Nevertheless, in both cases another requirement is that the legitimate interests of the person concerned are not contrary to the transmission. This requirement does not apply to transmissions more specifically provided for by law for an enumerated list of duties to inform, provided for by law or for requests of information by the intelligence services. In the latter case, transmissions of basic social data is permissible, although an official of the transmitting body with full legal education has to decide on this matter. Even stricter, basic social data needed for criminal proceedings may only be transmitted if a judge orders to do so. For the prosecution of major criminal offences (with a minimum punishment of one year imprisonment or other criminal offences of major interest), and if a judge orders to do so, even further social data may be transmitted. Some other possibilities for the transmission of social data are provided for by law, e.g. in the context of court proceedings about the duty to pay alimonies or the execution of sentences in such proceedings.

The information exchanges in the context of social law contain some structured information mechanisms according to art. VI-2 par. 1 of the ReNEUAL draft and consider certain duties to inform according to art. VI-2 of the ReNEAUL draft.

e) In the field of the public medical insurance system, a very recent act provides for the collection and transmission of specific data. This act was only passed on 9 December 2019, is in force, but not yet fully operational. According to this new act, the head organisation of the public medical insurances has the function of a data collecting point, to which the public medical insurance transmit, together with a pseudonym, data about every of their clients, especially age, sex, information about the insurance and data on the provider of medical services who balanced accounts. The data, including the pseudonym, is meant to make all insured persons identifiable for the public medical insurances. The head organisation of the public medical insurances checks the data received on completeness, plausibility and consistency and transmits them to a Research Data Centre (without the pseudonym) and a Confidential Authority (with the pseudonym). The Confidential Authority processes the received data, transforms the delivered pseudonyms into multi-period pseudonyms, and transmits a list of these pseudonyms to the Research Data Centre. This Research Data Centre has to provide access to its data for specific purposes to medical insurances, to their federal or state associations, to several research organisations, federal and state governmental departments that are responsible for the public medical insurance system and to head organisations of medical professions and of hospitals. These have to apply for the access to the data and, in the application, have to demonstrate that the purpose intended lies within the admissible purposes set up by the law.

The information exchanges which are being established by this law can be qualified as a database according to art. VI-2 par. 3 of the ReNEUAL draft.

f) In the field of alien law, the Residence Act contains specific provisions for the collection of personal data. It provides for the collection of necessary data by the aliens authorities and other public and private institutions performing supporting measures for return and reintegration and by the border police with regard to the departure. On request, public bodies with the exception of schools and other educational and care establishments for young people shall inform the authorities competent to enforcing the alien law of circumstances of which they become aware, as far as it is necessary for the purposes referred to with regard to the collection of data by these authorities. Additionally, public bodies shall immediately notify the competent aliens authority if, in discharging their duties, they become aware of specific circumstances, e.g. the residence of an alien without a permit or a suspension of deportation. In case of any other actions punishable under the Residence Act, the competent police authority may be notified instead of the aliens authority. Public bodies should notify the competent aliens authority immediately if, in discharging their duties, they become aware of special integration needs within the meaning of a statutory instrument enacted. The diplomatic missions abroad shall transmit to the competent aliens authority personal data on a foreigner which is suitable for establishing the latter’s identity or nationality, should they become aware that such data may be of current significance in enforcing the foreigner’s enforceable obligation to leave the federal territory. The bodies responsible for instituting and implementing criminal or administrative fine proceedings shall notify the competent aliens authority immediately that such crim-

inal proceedings have been initiated and that the criminal or fine proceedings have been settled at the public prosecutor's office, in court or at the administrative authority competent for prosecuting the administrative offence and imposing due punishment, stating the relevant statutory provisions.

The law also contains specific, more restrictive rules for the transfer of personal data restricted by other laws, of data in connection with integration measures and concerning the procedures to investigate, establish and document a foreigner's identity.

The law also establishes rules for the transmission of information by aliens authorities to authorities responsible to prosecute violations of rules for work (e.g. prohibitions of foreigners to work without a permit or without paying social insurances or taxes). The aliens authorities also notify the presence or departure of a foreigner to the authorities responsible for the population register. With the latter the aliens authorities, on a yearly basis, exchange regularly data on foreigners in order to maintain the respectively saved data up to date. This exchange may be accomplished automatically. An automatic exchange of data is provided for by the law also with respect to foreign missions and aliens authorities in visa proceedings.

The Federal Office for Migration and Refugees operates a Register of Temporary Protection from which, on request, the data may be transmitted to aliens authorities, foreign missions and other organisational units of the Federal Office for Migration and Refugees, including the National Contact Point established in accordance with Directive 2001/55/EC for the purpose of discharging their duties under the law on foreigners and asylum in connection with granting residence, allocating admitted foreigners to places of residence in the federal territory, relocating admitted foreigners to other member states of the European Union, reunifying families and promoting voluntary return.

The law provides for further rules on data transmission between the Federal Office for Migration and Refugees (as a National Contact Point) and competent authorities and institutions from other EU Members states under Directive 2001/55/EC on minimum standards for giving temporary protection in the event of a mass influx of displaced persons, the intra-community information under Directive 2003/109/EC on long term residents, the information exchange under Directive (EU) 2016/801 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing, regarding information to implement Directive 2009/50/EC on the conditions of entry and residence of third-country nationals for the purposes of highly qualified employment within the European Union and on information to implement Directive 2014/66/EU regarding the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer.

In addition, the law establishes a duty for information exchange between the aliens authorities and the customs authorities, the central commercial registry, courts, law enforcement and sentence executing authorities in cases of illegal employment. Such exchange also applies for the

security check of visa application data, which is collected at the Federal Office of Administration and is applicable for data collected by foreign missions from other Schengen member states, too. The data obtained in visa procedures is, by law, to be used for a comparison of data for security purposes.

These information exchanges in the field of alien law can be qualified as duties to inform according to art. VI-2 par. 2 of the ReNEUAL draft as they, triggered by specific discoveries, aim at informing the competent authorities about certain facts immediately.

The Asylum Act contains specific rules for information exchange in the asylum procedure. Identification measures are to be taken to verify the identity of foreigners requesting asylum by the competent authority, e.g. the Federal Office for Migration and Refugees. To do so they may only be photographed and the prints of all ten fingers be taken; foreigners below age 14 may only be photographed. In order to determine the foreigner's country or region of origin, the foreigner's oral statements may be recorded on audio and data media other than at his formal hearing. Such recordings may only be made if the foreigner is informed beforehand. These recordings shall be kept at the Federal Office for Migration and Refugees. The Federal Criminal Police Office shall assist in evaluating the data obtained for the purpose of establishing the identity. The Federal Criminal Police Office may not inform other authorities listed in the act why these records are being stored, unless other regulations provide otherwise. The Federal Criminal Police Office shall file data obtained separately from other identity records. The processing and use of data obtained shall also be permitted for the purpose of establishing the foreigner's identity or identifying evidence for purposes of criminal prosecution and threat prevention. The data may furthermore be used in order to identify unknown or missing persons.

These information exchanges can be qualified as structured information mechanisms according to art. VI-2 par. 3 of the ReNEUAL draft as they have specific purposes to which different authorities have to contribute although the Federal Office for Migration and Refugees stays the responsible authority.

The Federal Office for Migration and Refugees shall immediately inform the aliens authority of the district where the foreigner is required to stay or to take up residence of any enforceable deportation warning and shall immediately provide it with any documents required for deportation. The same shall apply if the administrative court has ruled that the suspensive effect of court action based on a reason precluding deportation shall apply only with regard to deportation to the country concerned and if the Federal Office does not continue the asylum procedure. The Federal Office shall immediately inform the aliens authority if the administrative court rules that the action brought against the deportation warning is to have a suspensive effect in cases. If the Federal Office delivers the deportation order to the foreigner, it shall immediately inform the authority responsible for the deportation of such delivery.

These information exchanges can be qualifies as duties to inform according to art. VI-2 par. 2 of the ReNEUAL draft.

Based on the Act on the Central Register of Aliens the Federal Office for Migration and Refugees operates, in co-operation with the Federal Office for Administration, this register. It has mainly four functions: it allows the authorities the storage and transfer of specific personal data for the identification of foreigners in the exercise of assigned duties (identification), access to information necessary for decisions and indication of authorities in possession of relevant information (evidence), information on relevant knowledge (substitution) and for statistical purposes. The register receives its data from the local aliens authorities, the Federal Office for Migration and Refugees, border police, criminal police (federal, state and customs), other police, prosecution service, courts, citizenship authorities, the Federal Work Agency and the local population register authorities. In determined cases, all these authorities have to report the data that is relevant in the specific context to the Central Register of Aliens. The law provides for the possibility of direct access to the register for the authorities that have to transmit data to the register in order to enable them to enter the data directly. In this case, they are obliged to correct immediately data that has become incorrect or of which it has been realised that it was incorrect. The responsibility for the admissibility of the transmission to the register rests explicitly with the transmitting authorities. They are obliged to report any corrections or objection by the person concerned. According to the general rules for the transmission of data from the register, a transmission is only admissible if the receiving public body needs the data to carry out its functions. As long as the request extends to other than basic data, the purpose has to be given in the request. The register authority has to deny the transmission if there are indications that the request might not be covered by the need for the functions of the requesting body. For the transmission of data of European Union citizens with the right of free movement, stricter rules apply as transmissions are only permissible to aliens authorities. The register authority has, in any case, to create records of any access to the register to enable checks, especially on the purpose of requests, the data transmitted and the identity of the requesting body. In a very detailed way, the law determines to which public bodies which kind of data can be transmitted. The law also explicitly provides for automatically generated release orders for an enumerated list of other administrative bodies. This concerns especially aliens authorities, police and intelligence services. If the possibility to access the register by automatically generated release orders is established the requesting authority will be responsible for the admissibility of any releases. The register authority, though, has to scrutinise the requests at random. Additionally, the law provides for an automated visa file, in which data of foreigners are saved when they apply for a visa. The foreign mission, border police and aliens authorities have to transmit the relevant data to this file. On request, data from this file can be transmitted to the police and aliens authorities. Automated release orders are permissible with regard to this file, too. The law also contains specific provisions on the rights of affected individuals, e.g. the right to be informed about the saved data, but also on certain exceptions from the rights granted to him/her by art. 15 GDPR as general rules. The law also contains specific provisions on the rights of correction, deletion, blocking and information of participating authorities. As rules for a specific area, they rank before general rules on data protection. As far as there are no specific rules in the law, the general rules on data protection are applicable.

The information exchanges in the context of this register can be qualified as operations of a database according to art. VI-2 par. 3 of the ReNEUAL draft, complemented by elements of a structured information mechanism according to art. VI-2 par. 1 of the ReNEUAL draft.

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.

We are not aware of any such mechanisms.

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 legal obligation to conduct impact assessments before introducing any information exchange. Yet, it is good tradition that some kind of impact assessment is done by the government before proposing any act to parliament, i.e. also before proposing the establishment of any information exchange mechanisms by law. How detailed these impact assessments are, depends on the individual case.

Additionally, yet rather from the perspective of reducing bureaucracy, there is a National Regulatory Control Council established by law that has the task to review the ministries' estimates of compliance costs for citizens, businesses and public authorities that is attached to the proposals of acts of the Federal Government. Part of these compliance costs is, as defined by the law, the costs of duties to inform.

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?

The case law on information exchange mechanisms in Germany is, to the best of our knowledge, limited. Although there is abundant jurisprudence that involves registers and databases or shared information, the information sharing usually does not constitute the main aspect of the case. The (shared) information is rather used to assess the cases among other information without the specific information being contested.

There are, for example, numerous cases of German administrative courts (although not the Supreme Administrative Court) in which the courts relied on information saved in the central

professional register when they had to review decisions of administrative authorities on the prohibition (or refused approval as far as required) of certain commercial activities (such as running a betting shop or collecting reusable material). One rather recent example is the decision of the Higher Administrative Court of Berlin and Brandenburg of 11.04.2019 (OVG 1 S 69.18 - ZfWG 2020, 79). Specific reference to the time limits in which the entries in the central professional register may be used to the disadvantage of a professional made the decision of the Bavarian Higher Administrative Court of 04.09.2018 (22 ZB 18.1165 - juris).

Similarly, there are abundant cases in which a person defends himself or herself against the withdrawal of his/her driving licence as ordered by the administrative authority. In many of these cases, the administrative decision is based on a number of violations of traffic rules, which are weighed according to a scheme of points (more points for more severe violations). The local traffic authority is informed by the central register on the violations of a person and of the points "collected" by him or her. When a specific number of points is reached, the driving licence is withdrawn. As past violations are deleted after a certain time, sometimes the dispute is about the time limits, but not about the transmission of data. For such a case, see for example the decision of the Higher Administrative Court of Saxony of 29.11.2017 (3 B 274/17 - NJW 2018, 1337) that also made special reference to the time limits.

In a case where the applicant was claiming the erasure of data in the Central Register of Aliens, the Federal Administrative Court stated in its decision of 22.02.2010 (1 B 21.09 - Buchholz 451.902 Europ Ausl- u Asylrecht Nr. 35) that the use of personal data that is inconsistent with European Union law does not constitute a right to erasure in an individual case. In order to guarantee the effectiveness of European Union law, the possibility to enforce rights according to the judgment of the (European) Court of Justice (of 16.12.2008 C-524/06) by an action for injunction is sufficient.

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.

In general, the administrative authority that has received data from another national administrative - be it by direct communication on request, be it as part of a transmission without request or be it by automatically generated release order from a register - may rely on the correctness of this data. As explicitly pointed out by a number of provisions on the responsibility for the correctness of the data transmitted, the transmitting body is responsible and has the explicit duty to inform about any changes or even about the fact that the correctness of data about an

individual is contested by the individual. Additionally, in some contexts, like.g. the Central Register of Aliens, the law demands explicitly that the register authority conducts a consistency check. Other provisions arrange for systematic crosschecks and comparisons of the data saved in central and local registers in order to identify and correct errors and to keep all registers up to date. Nevertheless, an administrative authority has to establish the facts of a case ex officio before taking a decision. This general rule is not questioned by the fact that in certain areas of law there is data transmitted by other public bodies, possibilities to obtain data from other public bodies upon request or registers containing data that could be relevant. On the contrary, these modalities constitute additional possibilities to investigate the facts of a case and thus extend the obligation to investigate. If, in the course of such an investigation, the administrative authority realises that there are pieces of information which do not match, it has to extend the investigation and question the correctness of the data given. In the end, the administrative authority which has taken a decision is responsible for this decision. If this decision is challenged in court, the administrative court itself has to establish the facts. If it finds the decision (partly) based on wrong facts, the decision is very likely to be quashed - with the usual consequences.

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?

As pointed out under a), an administrative authority that is preparing a decision has to establish the facts of the case ex officio. The obligation to investigate the facts includes consulting available registers and requesting information from other public bodies, always given that there are concrete hints that these paths of investigation might contribute to the establishment of the necessary facts for the specific proceedings. Thus, the administrative authority will obtain different elements of the facts from different sources. If such information is not consistent, e.g. if it does not "fit" to the rest of the factual findings, the administrative authority has to investigate further, to verify the one or the other piece of information.

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?

In general, the right of an individual to be informed about an exchange of his or her data between different administrative authorities stems from art. 15 GDPR. As far as a specific processing of personal data is not covered by the material scope of the GDPR according to its art. 2 para. 2, the German Federal Data Protection Act extends the applicability of the GDPR to any processing of personal data by a public body unless otherwise provided for in this or another act (sec. 1 para. 8). Nevertheless, departing from this general right of the individual to informed about any processing of his or her personal data, the German legislator has used the possibilities the GDPR leaves to the member states to modify this right to establish some further exceptions. According to sec. 34 para. 1 of the Federal Data Protection Act, the right of access according to art. 15 GDPR shall not apply especially in cases of national or public security and/or order, prosecution and prevention of criminal offences, the execution of criminal punishments or other important public interests. On the other hand, there are a few specific provisions which contain rights of individuals on access to data. As already mentioned in the answer to question I.1., the Act on the Central Register of Aliens contains a specific provision stipulating the right of the individual to be informed about the saved data. Similar provisions exist with regard to the driving licence registers. Yet, these provisions do not aim specifically at exchanges of data between public bodies, but at the substance of saved data.

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.

The liability for any damage caused by unlawful acts or omissions of public bodies is in general governed by sec. 839 Civil Code in connection with art. 34 Basic Law. The norm of the Civil Code still refers to the liability of a specific official who intentionally or negligently breaches the official's duty incumbent upon him in relation to a third party. With this (pre-constitutional) norm as a basis, the constitutional norm redirects the liability to the state or public body that employs him. Thus, the liability for damages caused by any public acts or omissions requires an official who intentional or negligent breach of an official duty. Also, the more specific norm in sec. 83

of the Federal Data Protection Act is based on this normative structure. Applying these rules to information networks or to false information entered into information networks, the probable solution by German law would be to analyse the specific legal framework of the information network or system concerned in the specific case. If there are, as it is common, legal duties to verify the transmitted or entered data, the defect in doing so might lead to the liability of the body which transmitted the data or entered it into a system. On the other hand, if the specific legal framework demands that the public body operating a register checks and verifies the data, the liability might rest with this body. This most probably would also be true in cases of malfunctioning of the register itself (e.g. because of software problems or other defects to the register as such). Nevertheless, it seems to be much more probable that damages related to data obtained from information networks or databases and the like are caused directly by a specific administrative decision, other act or omission in which this data has been used in one or another form. Taken into account the duty of administrative authorities to investigate the facts of a case themselves, it seems to be rather probable that in such a case the body this administrative authority belongs to is liable because the administrative body (most probably) could have verified the data. Whether there could be a certain compensation also depends on the specific legal framework and especially on the specific legal duties of the public bodies involved. Specific norms for this purpose do not exist, although art. 82 GDPR is, of course, relevant in the context of processing of personal data. It is noteworthy that sec. 83 of the Federal Data Protection Act does not provide for compensations, but does provide for the liability (towards the third person) of all of the public bodies that are involved in the automated processing of personal data in cases it cannot be determined which of them has caused the damage.

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?

As far as it is known, there are neither specific safeguards nor legal remedies of individuals in the German national legal order (i.e. additional to the GDPR) nor discussions about their introduction.

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?

In a case where the applicant was claiming for deletion of an alert for arrest warrant from the SIS, the Higher Administrative Court of Hessia stated in a decision of 10.03.2015 - 10 A 53/14 - (NVwZ-RR 2015, 712) decided that a person concerned can claim for a deletion of an alert inserted to the SIS by EU authorities before the German administrative courts. The full deletion is excluded when the alert as such is not false because the announced person is finally convicted for a criminal offence in another Schengen Member State. Neither art. 95 par. 2 sent. 1 nor Art. 112 par. 1 sent. 2 of the Convention implementing the Schengen Agreement (CIS) nor Council decision 2007/533/JI show rudimentary that in case of a violation of the general duty to scrutinize an alert must be deleted completely. Also under consideration of the data protection convention as established under art. 117 par. 1 CIS and Council decision 2007/533/JI it does not provide for a legal basis for a deletion claim if the alert is generally not to be rejected (like in the relevant case).

In a case against an expulsion order and a refusal of entry and stay, the Higher Administrative Court of Baden-Württemberg decided in a judgment of 19.07.2019 - 11 S 1631/19 - (juris par. 8 f.) that the observance of the duty of prior consultation before entering an alert for refusal of entry and stay under art. 28 Regulation (EU) 2018/1861 (SIS III) is not a procedural requirement for the issuance of an expulsion order.

According to the Higher Administrative Court of Northrhine-Westfalia, decision of 22.05.2019 - 11 A 0330/19.A - (juris par. 30), insufficient information of an asylum applicant in a Dublin procedure does not automatically establish the illegality of the administrative decision. It is up to the court to evaluate in the individual case if the challenged decision would be different without the alleged failure (with reference to CJEU jurisprudence on the consequences of procedural errors in judgments of 15. October 2015, C-137/14, EU:C:2015:683, par. 56, 60; of 7. November 2013, Altrip, C-72/12, EU:C:2013:712, par. 49, 53 f., of 10. September 2013, PPU C-383/13, EU:C:2013:533, par. 39 ff., of15. November 2011, Gibraltar, C-106/09, EU:C:2011:732, par. 179; of 5. October 2000, JAKO, C-288/96, EU:C:2000:537, par. 101 and of14. February 1990, Boussac, C-301/87, EU:C:1990:67, par. 31).
For the applicability of the CRAL to Union citizens with reference to the ECJ judgment of 16.12.2008 - C-524/06 see: Higher Administrative Court of Northrhine-Westfalia, judgment of 24.06.2009 - 17 A 805/03 - (AuAS 2010, 18-20).

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 Administrative Court Münster in a judgment of 26.06.2008 (8 K 52/07, juris par.58 f. and 64 f.) referred to the CJEU judgment in case C-503/03 in repeating that in a case when the family member of a third country national is entitled for freedom of movement under Community law, an alert for an entry ban is only admissible when the presence of that person constitutes a serious threat against a fundamental interests of society. Further on it recalled that under art. 5 par. 2 of the Schengen Implementation Agreement in case of an alert for an entry ban an entry must be denied in general. A contracting party may, e.g. on humanitarian grounds, deem it necessary to divert from this principle, so that the admission of the foreigner under alert tot he territory of this contracting party is limited and the other contracting parties are informed about this.

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.

In a judgment of 04.03.2010 (- 6 K 1371/09.W -, InfAuslR 2011, 173, par. 28) the Administrative Court Wiesbaden decided that the behaviour of an authority of another Member State must be attributed to the German authority even if the latter does not have responsibility under data protection law.

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).

As far as it is known, there are neither specific safeguards with regard to cross-border or multi-level information sharing in the German national legal order (i.e. additional to the GDPR) nor discussions about their introduction.