Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Spain

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.

It establishes certain exchange mechanisms such as:

1.1. Article 155 of Law 40/2015 , of 1 October, on the Legal Regime of the Public Sector: Transmission of data between Public Administrations: In accordance with the provisions of Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and in Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights and its implementing regulations, each administration must provide the necessary access to the remaining functional bodies, specifying the necessary conditions for the data protection and for reach the highest possible safeguards of security, integrity and availability.

Article 3 'General principles' of Law 40/2015, includes interoperability between the principles of action of public administrations, so that they will relate to each other through electronic means that ensure the interoperability and security of systems and solutions adopted by each of them, the protection of personal data, and will preferably facilitate the joint provision of services to data subjects.

1.2. The Law of the Public Sector Legal System, 40/2015, also provides for the establishment of a register which will allow for complete, reliable and public information on the number and types of public bodies and entities existing at any given time.

The duty of Co-Operation defines the cases in which assistance and Co-Operation may be refused by the requested administration, and the collaboration techniques are specified: The creation and maintenance of integrated information systems; the duty of assistance to respond to requests from other administrations for the best exercise of their powers and any other required by law.

A State Electronic Register of Co-Operation Bodies and Instruments, with its constituent effect, is hereby established in such a way that information concerning the Co-Operation and Co-Ordination bodies in which the General Administration of the State and its public bodies and entities are involved may be of general knowledge. Includes agreements are also in force at any given time.

The availability of increasingly integrated electronic mutual information systems (Market Unit Guarantee Law 20/2013, of 9 December) is enhanced.

1.3. According to Law 39/2015 of the Common Administrative Procedure, public administrations must obtain the documents electronically trough their corporate networks or through consultation with the data intermediary platforms or other electronic systems enabled for that purpose.

1.4. The Second Additional Provision of Royal Legislative Decree 1/1996, Law on Intellectual Property, in the version provided by Law 2/2019, dedicated to "Exchange of information between European competent authorities", provides for this mechanism and with respect to breaches committed by management entities established in another Member State of the European Union but providing services in Spain**:**

"1. The competent administration referred to in Article 155 shall, without undue delay, respond to requests for duly substantiated information made to it by a competent authority of another Member State in Connection with the application of this law, in particular the activities of the management entities or independent management companies which they are established in Spain.

2. The competent administration referred to in Article 155 shall give a reasoned reply within three months to requests made by competent authorities of other Member States of the European Union to take, within the framework of its powers, appropriate measures against a management entity which is established in Spain for infringements of this law which it has committed in the course of its activities in the requesting Member State."

1.3. *On 25 July 2018, Directive 2018/822/EC entered into force regarding the exchange of tax information relating to certain cross-border transactions*, also known as DAC 6 or the Tax Intermediaries Directive.

CCD 6 sets a period of approximately 18 months (until 31 December 2019) for the European Union Member States to transpose the guidelines set out in the Directive regarding the reporting obligation by tax intermediaries, and they must start to report certain cross-border transactions which are deemed to be abusive as from 1 July 2020.

On tax matters: Through the Information Exchange Agreements (AII), a channel for the exchange of tax information between tax authorities of States is established, which is key to the achievement of the objective of preventing tax fraud and evasion.

Information exchange agreements with Andorra, Aruba, Bahamas, Curaçao, Saint Martin and San Marino are currently in force, as well as the Agreement with the United States of America to improve international tax compliance and implementation of *the Foreign Account Tax Conversion Act - FATCA* (Foreign Account Compliance Act). Likewise, and on a multilateral basis, the Multilateral

Agreement between Competent Authorities on the Automatic Exchange of Financial Account Information is in force in Berlin on 29 October 2014.

1.6. Food Security: Reports of the Co-ordinated Information Exchange System (CIRI):

A coordinated system of food alerts is in place, the principles of which are based on Article 25 of Law 17/2011, on food safety and nutrition and Articles 50 to 52 of Regulation (EC) No 178/2002 of the European Parliament and of the Council laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety.

The Spanish Food Safety and Nutrition Agency (AESAN) draws up the Co-ordinated System for Rapid Exchange of Information reports annually which contain all the information relating to alert network notifications that affected our country, including a detailed description of the products involved, the hazards detected and the origin of the foods included in the notifications.

AESAN also produces various databases (food composition, business and food registration, etc.).

1.7. Law 41/2002 of 14 November on the basic regulation of patient autonomy and of rights and obligations in relation to clinical information and documentation provides that where necessary for the prevention of a serious risk or hazard to public health, health administrations may have access to patient identification data for epidemiological or public health protection reasons. Access shall in any case be by a healthcare professional subject to professional secrecy, with reasons given by the Administration requesting access to the data.

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.

The mechanisms in Spain can be included in the categories defined in Book VI.

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?
It is for the legislator to establish by law the legal basis for the processing of personal data by public authorities, but this legal basis should not apply to the processing carried out by public authorities in the exercise of their functions.

Article 28 of Organic Law 3/2018, of 5 December, on Data Protection (LOPD) stipulates that the controllers and processors must determine the appropriate technical and organizational measures to be applied in order to guarantee and certify that the processing is in accordance with the regulations, the organic law itself, its implementing regulations and the applicable sectoral legislation. In particular, they will have to assess whether the data protection impact assessment is appropriate, which is required in a number of cases where higher risks are assumed to exist and which require action to be taken. For example:

- Where processing could result in situations of discrimination, misused identity or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversion of pseudonymization or any other significant economic, moral or social harm to those affected;

- Also where processing would deprive the data subjects of their rights and freedoms or would prevent them from exercising control over their personal data; where processing is not merely incidental or incidental to the special categories of data referred to in Articles 9 and 10 of the Regulation and Articles 9 and 10 of the organic law itself or of the data related to the commission of administrative offences;

- When it involves an assessment of the personal aspects of the affected persons in order to create or use personal profiles of the affected persons, in particular through analysis or prediction of aspects relating to their performance at work, their economic situation, their health, their preferences or personal interests, their reliability or behavior, their financial solvency, their location or movements;

- When mass treatment occurs;

- Where the data are transferred to third states or international organizations for which an adequate level of protection has not been declared;

- And any others that the controller or processor believes may be relevant, and in particular those envisaged in codes of conduct and standards defined by certification schemes.

However, the LOPD does not differ in the case of public officers or not.

Law 39/2015, of 1 October, of the Common Administrative Procedure of the Public Administrations includes, amongst the rights of individuals in their relations with the Public Administrations, included in its Article 13, "to the protection of personal data, and in particular to the security and confidentiality of the data contained in the files, systems and applications of the Public Administrations". While security is amongst the general government policy principles, as well as the guarantee of the protection of personal data as established by Law 40/2015, of 1 October, on the Public Sector Legal Regime.

In response to the above, Article 156 of Law 40/2015 sets out the National Security Scheme (Esquema Nacional de Seguridad, ENS), which "aims to establish the security policy for the use of electronic means in the field of this Law, and comprises the basic principles and minimum requirements that adequately guarantee the security of the information processed".

The ENS is regulated by Royal Decree 3/2010 of 8 January, which was amended by Royal Decree 951/2015 to update it in the light of the experience gained in its implementation, technological developments and cyber threats and the international and European regulatory context.

Mandatory technical security instructions are essential to achieve adequate, uniform and consistent implementation of the requirements and measures contained in the Scheme and, in particular, to indicate how to act in specific aspects: Security status report; security incident reporting; Security Audit; Compliance with the National Security Scheme; Acquisition of security products; Employment Cryptography in the National Security Scheme; National Security Scheme Interconnexion and Outdoor Safety Requirements.

The National Security Scheme (ENS) pursues the following objectives: To create the necessary security conditions in the use of electronic means; to promote continuous security management; to promote prevention, detection and correction, to enhance resilience in the cyber -threat and cyber-attack scenario; to promote homogeneous security treatment that facilitates Co-Operation in the provision of digital public services when different entities participate; to serve as a model for good practices.

An orderly adaptation to the National Security Scheme requires the handling of the various issues, including the analysis of risks, including the assessment of existing security measures, and the preparation of an adequacy plan for improving safety.

Article 156 of Law 40/2015 also includes the National Interoperability Scheme (ENI) which "comprises the set of criteria and recommendations on the safety, conservation and standardization of information, formats and applications to be taken into account by public administrations for technological decision-making to ensure interoperability".

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?

STS of 16 July 2018, (ECLI: Es:TS:2018:2737): Agreement for the submission of letters and documents by telematic and electronic means to the various Common Registry and Distribution Services of the Courts of Madrid: Mandatory use of existing telematic or electronic systems. It does not infringe the right to an effective legal remedy. Legal service system through LexNet: There is no lack of control in data security and of any technical problems that may lead to a breach of the right to an effective remedy, of the right to equality before law, of the right to free competition and of the right to privacy and of the secrecy of communications.

STS of 9 October 2015, ECLI: Es:TS:2015:4224: The Royal Decree 640/2014, of 25 July, regulating the State Registry for Health Professionals, was challenged because it included the suspension or disqualification for the professional practise as a recordable figure. The Court is not satisfied that the authority of disqualification of non-corporate administrations is granted or entrusted to it when recognition is limited to sanitary administrations with competences linked to the purpose of the State Registry.

Judgement of 19 February 2018, Appeal No 82/2017, of the Court of Judicial Review Nº 3 of Zaragoza, which estimates the appeal filed against the resolution of the Directorate-General for Personnel and Teacher Training, requiring the appellant to provide negative certificate from the Central Registry for Sexual Criminals. The Royal Decree 1110/2015, which governs the Central Registry of the Central Sexual Criminals, was contested indirectly.

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 its Additional Provision Eight, entitled "Powers of verification of public administrations", the LOPD states that when applications are made by any means in which the data subject declares personal data held by public authorities, the body to which the request is addressed may carry out the checks necessary to verify the accuracy of the data in the exercise of his or her powers.

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?

There is no such obligation.

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?

Exceptionally, for example, data relating to infringements and administrative penalties. Article 27 of Organic Law 3/2018, on Data Protection, stipulates that this processing, including the maintenance of records related thereto, shall require:

A) The parties responsible for such processing are the bodies responsible for investigating the infringement procedure, for declaring infringements or imposing sanctions.

B) The processing is limited to the data strictly necessary for the purpose pursued by the data subject.

Likewise, Article 28 of Law 39/2015, referring to the documents provided by the interested parties to the procedure, stipulates that consultation or obtaining of the documents shall be presumed to be authorized by the persons concerned, unless their express opposition or the specific law applicable requires express consent. In the absence of any objection from the data subject, the Public Administrations must collect the documents electronically via their corporate networks or through consultation with the data intermediation platforms or other electronic systems enabled for this purpose.

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

Article 11 of the Spanish Personal Data Protection Act provides that when personal data have not been obtained from the data subject, the data controller may comply with the duty of information established in Article 14 of Regulation 2016/679 providing the data controller with the basic information set out in the preceding section, indicating an electronic address or other means that provides easy and immediate

access to the other information. This refers to the identity of the data controller, the purpose of the processing and the possibility of exercising the rights set out in Articles 15 to Articles 22/679 of the Regulation (2016). In such cases, the basic information shall also include: (A) The categories of data to be processed. B) The sources from which the data originated.

But this is not always the case. For example, pursuant to the aforementioned additional provision , the tax authorities responsible for the data files with a tax credit as referred to in Article 95 of Law 58/2003 of 17 December, General Tax, may, in relation to these data, refuse the exercise of the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679, where the same would hamper administrative actions to ensure compliance with tax obligations and, in any event, where the latter would be affected.

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.

Pursuant to articles 70 and 77 of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights (LOPD), the controllers and processors will be responsible for processing

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

Yes. Articles 13 to 18 of the LOPD set out the rights of access, rectification, erasure, restriction of processing, portability and opposition. The existence of political or academic discussion on the required issues, and the existence of a recent legislative proposal on this subject, are matters that exceed the scope of the Court's knowledge.

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?

There is no record of the issuance of judgements in relation to the question raised. There are no ongoing procedures regarding the subject concerned.

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.

With regard to Case C-503/03 Commission v Kingdom of Spain (2006), on the date of reply to this questionnaire the Supreme Court of Spain has not delivered any judgement based on the case-law of the CJEU. Other courts have done so in the cases listed below:

ECLI:ES:TSJPV:2016:3090; ECLI:ES:TSJPV:2014:2631; ECLI:ES:TSJPV:2013:2846; ECLI:ES:TSJCV:2010:2541; ECLI:ES:TSJCV:2009:6987; ECLI:ES:TSJCV:2009:3310; ECLI:ES:TSJCV:2007:5403; ECLI:ES:TSJM:2019:210; ECLI:ES:TSJM:2017:13730; ECLI:ES:TSJCV:2017:7941; ECLI:ES:TSJPV:2013:3028; ECLI:ES:TSJM:2011:13266; ECLI:ES:TSJPV:2010:5421; ECLI:ES:TSJCV:2010:1753; ECLI:ES:TSJPV:2010:3925; ECLI:ES:TSJM:2008:26402; ECLI:ES:TSJPV:2007:2161; ECLI:ES:TSJPV:2007:2165; ECLI:ES:TSJPV:2007:2148; ECLI:ES:TSJPV:2007:1709; ECLI:ES:TSJPV:2007:1108; ECLI:ES:TSJPV:2006:2632; ECLI:ES:TSJPV:2006:1385; ECLI:ES:JCA:2012:2271, ECLI:ES:JCA:2012:2592; ECLI:ES:JCA:2012:2268; ECLI:ES:JCA:2012:2258; ECLI:ES:JCA:2012:2226 y ECLI:ES:JCA:2011:187.

While it is necessary to clarify that the appointment of case C-503/03 refers to a requirement that foreign conduct constitutes a genuine and sufficiently serious threat to expulsion, rather than to include it on the list of alerts that are not admissible under the automated SIS II information exchange system.

In relation to art. 25.2 of the SIS II Regulation (EC) 1987/2006, there is no record of the issuing of judgements in relation to the case-law of the CJEU regarding this provision.

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?

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).

No. The existence of academic discussion on the matter and the existence of any legislative proposal in this respect goes beyond the jurisdiction of the Court.
