Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Italy

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).

Definitions
VI-2 Definitions

(1) A structured information mechanism means a pre-defined workflow allowing authorities to communicate and interact with each other in a structured manner beyond the general obligations of mutual assistance according to Book V.

(2) A duty to inform is an obligation for an authority which exists under EU law to provide data or information to another authority without prior request.

(3) Database means a structured collection of data supported by an IT system and managed by a public authority, which provides at least one other competent authority at EU or Member State level with access to stored data without prior request.

(4) An information system is either a specific software or IT infrastructure (IT system) or an organizational infrastructure supporting inter-administrative information exchange or establishing a database.
(5) Participating authority means any authority taking part in an information management activity within the scope of this book, be it as a competent authority, a contact point, a management authority, a verification authority or a general supervisory authority.

(6) `Data supplying authority´ means a competent authority supplying data to other competent authorities according to a duty to inform or entering data into a database.

(7) `Person concerned´ means any natural or legal person identifiable, directly or indirectly, by reference to data exchanged or stored by an information management activity within the scope of this book.

Duty of sincere cooperation

(1) Public authorities using an information system shall ensure the efficient functioning of the system within their jurisdiction.

(2) Public authorities using an information system shall ensure effective communication between themselves and with the Management Authority.

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? <u>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.</u>**

We refer to the definition of information exchange consistent with that described by RENEUAL Model Rules Book VI.2.1. *(1) A structured information mechanism means a pre-defined workflow allowing authorities to communicate and interact with each other in a structured manner beyond the general obligations of mutual assistance according to Book V.*

More specifically, we have investigated information systems as defined by RENEUAL Model Rules Book VI.2.1. We have tried to distinguish, as requested, between

(1) information exchanges within mutual assistance regimes, where there is a requesting authority that is asking for information and a requested authority performing an administrative task, and

(2) information exchanges that materialize as the execution of pre-existing duties of information without a prior request.

Many definitions, relevant for the questionnaire and the comparison with Reneual Rulebooks, are provided by the Italian Code of digital administration (CDA). The Code of digital administration (CDA) was enacted in 2005 and it has been modified over the years to adapt to technological changes. Technology has not been the only driver of change. The increasing correlation between digitalization and bureaucratic simplification has generated further modifications which bear consequences over the issues raised in the questionnaire.

The scope of application of CDA is defined by article 2 and it refers to public administrations, including both central and local. The CDA establishes a principle of free accessibility of administrations to data produced by other administrations (see in particular artt 47, 50, 58 and 60, 7). A similar principle has been established also for individuals.

These principles of free accessibility must be coordinated with those related to access regulated by the general law on administrative proceedings l. 241/1990 art. 22. In particular art. 22, paragraph 5, of the general law on administrative proceedings, addressing the access by public administrations, frames exchange of information within the general principle of loyal cooperation which is also regulated by Reneual Book VI rule 5.

In general terms, but for the rules on data protection and those of ciber security, the free flow of data and its full accessibility characterizes both the exchanges among administrations and the access by private actors to data sourced by the administration.
As a general matter there is similarity but not perfect coincidence between the Reneual definitions and those provided by CDA (see for example the definition of data base provided by Reneual Rule VI.2.3 and that of art. 60 CDA).
In particular, article 50, paragraph 1, CDA provides that data of public administrations are created, collected, stored, made available and accessible through the use of information and communication technologies that allow their use and reuse.
Art. 50, paragraph 2 states also that "*Any data processed by a public administration - excluding those relating to the functions of public order and security, national defense and security, judicial police and economic-financial police and electoral consultations, as well as to emergency and alert communications in the field of civil protection, and in compliance with the legislation on the protection of personal data - is made accessible and usable to other administrations when the use of the data is necessary for the performance of the institutional tasks of the requesting administration, without charges for the latter, except for the provision of additional processing*."

The third paragraph of art. 50 also provides that public administrations, in the context of their institutional functions, analyze their data in combination with those held by other public administrations, without prejudice to the limits referred to in paragraph 1. The rule provides that this activity is carried out according to the methods identified by the Agency for Digital Italy (hereinafter AgID) with the Guidelines. These guidelines have not yet been adopted.

Information and data are exchanged in different ways. Among these, the public Connectivity and Cooperation System (SPC) referred to in art. 73 of the CAD. The SPC is a set of technological infrastructures and technical rules that ensures the interoperability between the information systems of public administrations, allows the informative and IT coordination of data between central, regional and local administrations and between these and the European Union systems. Access is open to public service providers and private entities.

For the purpose of making this interconnection effective, the new Digital National Data Platform is currently being tested (see https://teamdigitale.governo.it/it/projects/daf.htm).
However, given the time and space constraints, it is beyond the scope of the respondent a comprehensive examination of the similarities and divergences between Reneual rule books and the definitions in C.D.A.

National legal systems engage into information exchange by managing information and data. Exchanges occur among central administrations (horizontal) and between central and local administrations (vertical): within the vertical dimension there are exchanges between the central authorities and local units subject to hierarchical power and exchanges between central and local administrations that are not embedded in a hierarchical relationship.

Often these exchanges have both a national and an EU dimension. We have tried to identify systems with a dual dimension to verify how the EU principles and the internal principles correlate. The conclusion is that information exchanges among administrative authorities of different countries might not coincide with those within each country as to management responsibility, system to control the truthfulness and reliability of information, liability towards third parties. Often, as it is the case for the Schengen information system, internal procedures remain within the domain of contracting states and the uniformity of technical protocols ensure interoperability in order to warrant access by each administration to the exchange system. Allocation of responsibility is often a consequence of the different procedural administrative rules followed by each MS or contracting state.

The analysis below addresses three main issues:

1) Cooperation in data collection, exchanges among authorities, and consequences for lack or failed cooperation.
2) Data management when they are false or altered and necessitate modification or deletion.
3) Liability towards third parties for false or inaccurate information and for violation of GDPR (Regulation on data protection 679/2016).

The creation of information exchange systems (IES) among administrations is based on the duty of loyal cooperation. One of the objectives of cooperation is to reduce the administrative burdens for citizens and for enterprises. The creation of a single source of data, of electronic cards, permits citizens to access data sourced by several administrations and to interact with multiple administrations at once. Simultaneous rather than sequential interaction is the preferred mode of operation.

One key dimension of the regulatory regime is the relationship between information exchanges and administrative decision making. How is the administrative decision-making modified depending on the architecture of information exchanges? More specifically how is the procedural structure and the participation of private actors modified by the use of information exchanges that may transform the architecture of organizational (administrative) interaction?

An interesting evolution, likely to have an impact on the issues dealt with in the questionnaire, is the use of algorithms in administrative decision making. The Italian Council of State has issued two judgments in 2019 where the use of algorithms has

been considered (Cons. Stato n. 2270/2019, Cons. Stato 8474/2019). It has recognized the benefits of algorithms for automated decision making by the administration. At the same time, it has defined the boundaries and the degree of transparency associated with the use of algorithms. The principles stated in those judgments are applicable a fortiori to automated information exchanges taking place among administrations with the aim to simplify and speed administrative decision making. For the limits of automated administrative decision making when they are the outcome of an information exchange it is necessary to consider art. 22 of GDPR stating the general principle *"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".*
The collection of data operates within the umbrella of the duty to sincere and loyal cooperation. IES data must be based on standardized protocols. Administrations must comply with technical standards of the quality and form of the exchanged information. Standards concern how information are collected, processed, modified and deleted.

We now provide some anecdotal illustrations of information exchange systems (IES) regulated by specific legislation

1 ANPR

- The national registry office for population (ANPR) is a data base that collects data concerning residents in Italy. It sources from the databases of 7954 towns. The responsible administration of the program is the Ministry of the Interior. The technical manager is SOGEI, a company owned by the Ministry of economy. The data base is the result of the cooperation of almost 8000 towns under the coordination of the Ministry of interior and the beneficiaries are other administrations and private parties who can access the database. The database offers services to the towns and to other administrations. In particular three groups of services can be identified: registration services, advisory and requests by the administration and data extraction, certification services for administrations and for individuals. It is difficult to use only one of the definitions provided by Rulebook VI.2. The ANPR can in theory fit with the definition of a structured information system under 1, a data base under 3, and an information under 4.

- The electronic medical record (health folder)

The decree "Regolamento recante procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio Sanitario Nazionale, anche quando gestiti da diverse amministrazioni dello Stato" defines the procedures to interconnect at national level informational systems of the regional systems within the national health care system. This interconnected system coordinates and integrates other information systems that operate at regional and local level. It should be reminded that health care is an area primarily within Regional competence in Italy.

The main functions of the system are:

- keep records of the medical conditions of each patient.
- Monitoring fundamental levels of health care assistance.
- Statistics by public administrations.

The administration responsible is the Ministry of health.

The European professional Card

The European professional card (EPC) is available from 18 January 2016 for five professions (general care nurses, physiotherapists, pharmacists, real estate agents and mountain guides). It might be extended to other professions in the future.

"The EPC is an electronic certificate issued via the first EU-wide fully online procedure for the recognition of qualifications. This digital procedure is based on the Internal Information system (IMI) and allows professionals to communicate with the relevant authorities inside a secure network. The IMI also provides for an official, multilingual communication channel between the regulating authorities for professionals in EU countries to facilitate their cooperation and enhance mutual trust. The EPC does not replace the 'traditional' recognition procedures under the Professional Qualifications Directive, but it does offer an advantageous option for professionals who wish to work either temporarily or permanently in another EU country."

The EPC encompasses both cross-border transnational administrative cooperation and internal cooperation between various administrations. Different ministries, depending on the profession, have the responsibility of data collection and processing.

In Italy significant case law has developed in relation to phisiotherapists.

The Commission Regulation states : "

(8) The EPC procedure can lead to the adoption of different types of decisions by the competent authority of the home Member State or of the host Member State. It is therefore necessary to define the possible outcomes of an EPC procedure as well as to specify, where appropriate, the information to be included in the electronic document stating the outcome of the EPC procedure.

(9) To facilitate the task of the competent authority of the host Member State and to ensure that the verification of an issued EPC by the interested third parties is easy and user-friendly, it is appropriate to provide a centralised, online verification system of the authenticity and the validity of an EPC by the interested third parties that have no access to the IMI. That verification system should be separate from the online tool referred to in Article 4b(1) of Directive 2005/36/EC. Such verification of the EPC should not provide access for interested third parties to the IMI.

(10) In order to ensure data protection in relation to the application of the alert mechanism, it is necessary to specify the roles of the competent authorities handling incoming and outgoing alerts and the functionalities of the IMI in withdrawing, modifying and closing alerts and ensuring the security of data processing." (Commission implementing Regulation 2015/983 of 24 June 2015 on the procedure for issuance of the European Professional Card and the application of the alert mechanism pursuant to Directive 2005/36/EC of the European Parliament and of the Council).

The case law concerning the application of the Regulation to applications for the EPC sent to the host state via the IMI system raises a number of issues. The electronic procedure unlike the manual does not include suspension of the time in case of the necessity for clarifications. Accordingly time runs and if the adminstration does not issue a decision after two months, the legal assumption is that the application has been accepted and the professional can exercise.

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.

For reasons of time and space it is beyond the scope of the analysis to test the compatibility of the schemes and programs with RENEUAL categories.

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?

If no personal data is involved, no.

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 clarifies the correlation between information systems, cooperation among administrative authorities and procedural simplification of administrative activities (TAR LAZIO 12760/2019).
The exchange of information is regulated by the duty of loyal cooperation, a general principle within the framework of the good administration. The duty of loyal cooperation regulates the relationship among administrations in the interest of the final beneficiary of administrative activities.
Information exchanges systems (IES) are changing administrative decision making especially when the final decision depends upon the cooperative interplay of several administrations occurring through information mechanisms. The case law is reinterpreting the rules on preliminary investigation (istruttoria procedimentale) in the light of the architecture of information exchange systems. In a similar vein the scope and extent of grounds related to administrative decisions, taken on the basis of digital information exchange systems, has been revisited (TAR LAZIO 2775/2014). Technical shortcomings associated to the information system, cannot constitute a justification for the rejection of the citizen's request; the administration in charge of the final decision is obliged to overcome those problems and ensure effective and fair proceedings.

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.

The answer to this question is based on a limited number of regimes that have been examined. No general principles have been established by the law and the case law is highly underdeveloped.
The exchange of data among administrations is based on the principle of mutual and loyal cooperation. The definition of this duty mirrors that of the duty of sincere

cooperation under art. 5 of Reneual book VI with some relevant nuances whose examination is beyond the scope of this analysis. The Italian legal system correlates these exchanges to the objective of simplifying administration action in the interests of citizens and economic actors. The CDA has established a system of connectivity based on the interoperability among databases of each administration (art. 2 CDA). The transfer of data does not result in a transfer of ownership (art. 50.3 CDA). The transferor remains in control of data and holds the associated responsibility. This rule marks a difference with that of data protection where the transfer of data may result in a potential modification of both the data controller and the data processor depending on the purpose of data processing of the issuing and the receiving administration.

The existence of a duty to scrutinize data sourced by other administrations should be evaluated in the light of each administration legitimate reliance. Absolute reliance implies no duty to scrutinize and puts the liability on the administration providing data. Reasonable reliance is associated with a limited duty to scrutinize the accuracy and truthfulness. No reliance implies a full scrutiny by the user and no liability on the data collector.

The first case occurs when the collection of data is the execution of a legal duty. The second occurs when data collection is the exercise of a power e.g. when the administration collects data in order to perform its tasks and then the data are transferred or used by other administrations for their own activities.

The question posed can be further subdivided into two different sub-questions: whether there is a duty to scrutinize and whether there is a power to scrutinize. We examine them in turn.

Verification of information has several dimensions: truth, accuracy. At the national level the principle is that of mutual trust among administrations so that each administration can rely on the accuracy of the information provided by other administrations according to the principle of loyal cooperation. The same principle applies for the decision making body, being a platform or a data-base. When an administration has the legal duty to collect, process and verify the information the decision making body and the other administrations can rely upon them and **there is no duty** to scrutinize the truthfulness and the accuracy of information and data. When, instead, the collection of information and their provision does not constitute the implementation of a legal duty then the applicable principle is that of reasonable reliance.

When several administrations provide information is there a power to verify that accuracy? In the latter case the issue is whether the scrutiny may represent a violation of the administrations' competence.

When there is a legal duty not only the other decision-making body and the other administrations do not have the duty to scrutinize but also they would not have the power to scrutinize. When, instead, the collection and provision of information and data

is not the execution of a legal duty the other administrations have the power to scrutinize the information and verify its accuracy and truthfulness.

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?

The answer to this question is based on a limited number of regimes that have been examined. No general principles have been established by the law and the case law is still underdeveloped.
A duty to scrutinize the information may arise in relation to several circumstances when there is a need for a consistency check among data sourced by different administrations.

- When final data are the result of processing other data coming from various sources and different administrations.
- When the data are manifestly false.

This consistency control takes place, for example, in the data-base concerning residency (ANPR above) where, according to the platform, the same citizen is resident in more than one town. Clearly, this result is contradictory and requires a consistency check. This consistency check is among homogeneous data and must be performed by the data processor. Consistency checks can also occur among heterogeneous data as it happens when a subsidy is conditional upon requirements both of fiscal and personal nature (income, residence, ect.) as in the social card program. Similarly, in the telematic driver counter program (sportello telematico automobilistico) where car ownership and authorization to circulate for the vehicles are issued and a consistency check is required by the decision making body managing the platform between data concerning the car ownership and data concerning the identity of the owner.

The exercise of the duty to scrutinize is regulated by negligence standard defined by art. 2043 of the Civil Code. What is the standard for scrutiny? The standard is that of the duty of care. The decision making body has a duty to verify and the standard to comply with is due care (Consiglio di Stato, sez. IV, 1827/2019). Once the scrutiny has occurred the scrutinizing administration has the obligation to refer or to correct depending on whether it is or it is not the decision making body.

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

The answer to this question is based on a limited number of regimes that have been examined. The case law is rather underdeveloped.

The common principles are established by Regulation 679/2017 (GDPR) artt.. 13 and 14 and it is therefore uniform across Member States. The Italian data protection (privacy in the ordinary language) code has been modified in order to implement GDPR. The Privacy code enacted to implement EC directive 46/96 has been modified in order to comply with EU Regulation 679/2016 (GDPR) with the Italian legislative decree 101/2018. The privacy code, in its new version compliant with GDPR, has not yet been fully coordinated with the CDA. The coordination between CDA and the code poses many problems but is beyond the scope of the analysis of this questionnaire to explore the lack of proper coordination between the two statutes.

The general rule based on hierarchy is that in case of conflict Regulation 679/16 prevails on CDA. As we shall see the general principle is that communication among administrations can take place without consent only if it executes a legal or regulatory norm. Yet when it is instrumental to the performance of a public interest tasks as those listed by the Privacy Code a communication to the Data Protection Authority that is not followed by contrary indications within 45 days allows the communication and the exchange even without a specific legal rule conferring the power.

A more complex issue concerns the allocation of control and liabilities among data controllers and data processors when multiple administrations participate in data sharing and processing.

According to GDPR art. 4 (7) | *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; (8)* | *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

The general principle to identify the controllers and distinguish it from the processors is related to the purpose and the objective pursued by the conferring and the receiving administration in an exchange information system (see the decisions of the National Data Protection Authority). If they pursue different institutional objectives they should be both considered controllers. If the receiving administration pursues the same objective as the conferring one it might be considered a processor, unless the modes of processing are such that they amount to an independent processing. In the latter case the receiving administration could be considered, according to RENEUAL

language, a decision making body and held responsible as a controller rather than as a processor. The qualifications matter not only internally for the relationships among administrations but also in relation to the rights of the data subject.

In conclusion, the general principle is that the administration providing the information and responsible for the program is the data controller and the administration in charge of the management of the platform or the database is the data processor when the purpose of data use is the same (art. 28 GDPR). When, instead, the receiving administration uses the data for a different purpose it becomes the controller.

When the purpose is jointly determined, the administrations are joint controllers**.** According to art. 26 GDPR 1. *Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.*

Hence, when there is joint control administrations can allocate responsibilities through agreement but the data subject can seek remedies with each of them. The internal arrangement is not binding on interested third parties.

Having stated the general principle, the analysis of individual programs concerning digital information exchanges suggests that lines are not bright but blurred. When there are multiple sources of data is each of them a data controller? If the data go into a single platform when are the administrations joint controllers?

There is not a single solution. Whether there is a single or joint controllers depends on the architecture of the IES. It depends on both the architecture of the platform and the relationship among the administrations providing data**.**

In some instances, centralization of data implies that a single data controller exists. In the case of ANPR for example the Ministry of Interior is the data controller and the individual mayors of each town are considered data controllers only for the data they have provided but no joint controller mechanisms has been set in place. The Ministry is a data controller for data storage, communication and security, the mayors are data controllers for data registration. (*Circolare 1/2015 Pubblicazione del d.P.C.M. 10 novembre 2014, n. 194 (Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR).* Technically they are NOT joint controllers.

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

The reference to answer this question is art. 22 GDPR where the following principle is stated:
" *1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.". Then paragraph identifies the exceptions" Paragraph 1 shall not apply if the decision: (a) | is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) | is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) | is based on the data subject's explicit consent".*

The general principle is that no consent is needed when data are transferred from one administration to another and the purpose for using the data is the same. The rules concerning consent have been abrogated (former art. 81) and now the principle is that a single communication is sufficient (art. 80). Exceptions concern health, where the transmission of data is subject to the information and consent according to the art. 78 and 79 of the Data Protection Code.
The Art. 2 ter of Legislative Decree No. 196 of 2003, as amended by Legislative Decree no. 101 of 2018 (Privacy Code) provides that the legal basis envisaged by article 6, paragraph 3, letter b) of the regulation consists exclusively of a law or, in the cases provided for by law, regulation.
For the exchange of data between public administrations, where personal data are involved, the second paragraph of art. 2 ter provides that the communication between owners who process personal data other than those included in the particular categories referred to in article 9 of the Regulation and those relating to criminal convictions and crimes referred to in article 10 of the Regulation, for the execution of a task of public interest or connected to the exercise of public authority is allowed if provided for in paragraph 1. In the absence of such a rule, communication among administrations is allowed when it is necessary to perform public interest tasks and of institutional functions. The art, 2 sexies of the Privacy Code makes a very long and detailed list of illustrations of the public interest activities within such as for example the storage of data concerning residence referred to for the management of ANPR.
When one of the public interest function has to be performed by multiple administrations, communication can be operationalized if the forty-five-day period has elapsed from the relevant communication to the national Data Protection Authority and no objections or indications of alternative modes have been provided for.

Vice versa, pursuant to paragraph 3, the dissemination and communication of personal data, processed for the execution of a task of public interest or connected to the exercise of public powers, to subjects who want to treat them for other purposes are allowed only if provided for in paragraph 1.
According to the paragraph 4 of art. 2 ter of the Privacy Code communication among various entities including communication among public administration includes consultation and interconnection. This definition encapsulates an information exchange system as characterized by Reneual Rule book VI.

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?

There is a difference between the French and the English version since in the French the term is “droit opposable”, whereas in English text the term is “enforceable”. We follow the English version; the answer is affirmative and based on the interpretation of GDPR. When the process is not automatic the right to be informed is legally enforceable. As indicated before the right to be informed is not instrumental to the expression of consent, that is not required. The right to be informed is instrumental to the possibility to exercise the other rights listed in artt. 15/22 GDPR.
In particular according to art. 21 GDPR concerning the right to object 1. *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*
The public interest exception is stated in paragraph 6 of art. 21 GDPR
6. *When personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89 (1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*
The rule is applied without changes in the Italian legal system.
When the information exchange is automated the data controller has a duty to ensure full compliance with the rights of the data subject to have an interaction with the administrations participating in the information exchange. See art. 21 GDPR “3. *In*

the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

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 main issue is the definition of liability for data gathering and for effective exchanges. The liability can stay with each administration, can be conferred to one of them responsible for the gathering or to a third party that is contractually allocated the task to manage the exchange.
The allocation of liability among the administrations may be regulated by law or contractually.
Clearly there is a correlation between the answers provided for under question 5 and the answers to this question. Depending on the degree of reliance the liability regime changes.
It will be exclusively on the administration providing data when the reliance of the receiving administration is complete.
It will be distributed between the providing and the receiving administration when reliance is only reasonable. Art. 2055 of the Italian Civil code defines rules for allocating liability among multiple tortfeasors.
It will be exclusively on the receiving administration when no reliance is admissible.
Ownership of data also matters to establish liability. Pursuant to the art. 1, paragraph 1, lett. cc, of the CAD, is the "owner of the data" is the public administration that originally formed for its own use or commissioned to another subject the document that represents the data, or that has the availability. Art. 50, paragraph 3 bis, of the CAD specifies that the transfer of data from one information system to another does not change the ownership of the data.

In the event of illegitimate administrative activity due to incorrect data handling or evaluation, the national rules on the non contractual liability of the public administration (tort) apply.
The general principle when it is regulated by the law is that liability stays upon the administration for the accuracy and truthfulness whereas the liability is on the decision making body for processing and updating the information and the data.
To conclude, pursuant to the art. 2043 of the Civil Code, the public administration is required to pay compensation for the unjust damage caused by its illegitimate activity. See for an example the judgment by T.A.R. Lazio Roma Section III ter, 03-06-2019, n. 7097.

The contractual allocation of liability is free within the limits of GDPR. The examples we have found tend to place the liability upon the individual administrations and not on the decision making body. For example liability is contractually regulated in the case of Alma Laurea (an Italian electronic platform concerning graduates data) where universities have to confer data concerning graduates placement and the liability concerning the accuracy of data is determined contractually in the consortium contract. The contractual term exempts the consortium (the decision making body responsible for the exchange) from liability concerning the choice of information provided and their truthfulness and accuracy.

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?

The remedies differ depending on whether the individuals are claimig that data are false or that the information exchange is illegal or whether a violation of the rules on privacy and data protection have occurred. Administrations can regulate internally the allocation of liabilities but the private actor has a right to claim against each participating administration. The general principle is that internal allocation of control and liabilities cannot produce effects on third parties especially if those effects reduce or prevent from exercising fundamental rights.
To the best of our knowledge there is no legislative proposal on this question.
Currently there are no political or academic discussions about further needs for new or more specific legal safeguards in this context, and there are no recent legislative

proposals on this topic. The case law is too underdeveloped to generate a debate on a potential legal reform.

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?

According to the wide majority of Italian case law applying the Schengen Convention the national administration is bound to the SIS alert issued by another State and, consequently, does not have any obligation to motivate and to scrutinize the accuracy and the grounds of the alert but in case of factual mistake or bureaucratic mishap (Council of State n. 3421/2017). The principle of mutual trust requires deference to the evaluation carried by the other administration unless serious reasons require additional investigation. Mutual trust prevents States from engaging into a scrutiny of the activities of other administrations unless there is serious evidence that fundamental rights might be violated.
Nevertheless, in a small number of cases, it has been stated that the obligation of motivation must be fulfilled by informing the addressee of the negative administrative decision. Information should at least provide the details of the SIS alert. This information would be necessary in order to give him or her the possibility to oppose the alert before the authority which has issued it and defend him or herself. (T.A.R. Roma, (Lazio) sez. II, 23/04/2012 n.3658).

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?

On the CJEU judgment Commission v Kingdom of Spain, there is a very limited number of relevant cases. The administrative courts, when referring to the CJEU judgment on

request by parties, have never applied it, because the cases were not concerning spouses of a European citizens. (T.A.R. Lazio Roma Sez. I quater, Sent. 19-04-2013, n. 3989).

On the contrary, Civil Court of Cassation (Section I, of 14 November 2008, n. 27224), which is competent in such cases, has resorted to this judgement in order to establish whether, once the applicable legislation has been identified, the competent administration can reject the visa application, citing exclusively for the purpose of refusing the notification for the purpose of refusing entry within the Schengen area. The Board believes that this question should be answered in the negative.

In the grounds of the judgment, the Italian Court of Cassation recalled that, according to the European Court, there is a burden for the national authorities of the EU Member States to verify whether the presence of third-country nationals, spouses of citizens of Member States of the 'European Union, constitutes a real, current and quite serious threat to a fundamental interest of the community. It follows that the Member State (in the case decided by the aforementioned ruling, the Kingdom of Spain), where it refuses entry into the Schengen area to citizens of a third State who are spouses of citizens of a Member State, for the sole reason that they are reported in the SIS for the purpose of non-admission, without first verifying whether the presence of such persons constitutes an actual and sufficiently serious threat to a fundamental interest of the community, violates the obligations imposed on it under the Articles. 1 - 3 of Directive 64/221.

In this case, given that the refusal of the visa was made on the basis of a mere report for the purposes of refusing entry, it must be considered that the alleged violation has occurred.

Regarding to the art. 25 of the Convention, the administrative courts have sometimes referred to it, on request of the parties, but they have not applied it.

For example, in some cases, it has been stated that there is not any obligation for the administration to scrutinize why the alert was issued by another State, except when the residence permit was requested for humanitarian reasons, national interest of to fulfil the international obligations of the State, under the article 25 of the Convention. Nevertheless, the decided case was not dealing with these exceptional situations. (T.A.R. Firenze (Toscana) (sez. II, 29/06/2011, n.1123 and T.A.R. Roma, (Lazio) sez. I, 11/12/2009, n.12799)

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. To the best of our knowledge there is no any case law on this matter.

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).

N/A