Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Cyprus

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

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

11 May 2020

Bundesverwaltungsgericht (Federal Administrative Court), Leipzig

Questionnaire

Introduction:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Since the rapid technological advancements have accelerated the establishment of information exchange systems throughout the governmental sector numerous national information systems are in use today. Public authorities nowadays, have integrated these systems in the decision-making process, either wholly or partially, at different stages of the process, in order to facilitate their administrative needs. They, undoubtedly, play, an important role in the administration since they can be used to aid or guide a human decision-maker or they may, even, be used in lieu of a human decision-maker. More so, these systems provide the opportunity for interconnections, exchanges and sharing of information and data.

In Cyprus, such an exchange system exists under the name of Government Data Warehouse (“GDW”) which is an innovative national information exchange system. The GDW is a central repository of government data. It is a single cohesive database with a subject-centric approach, in order to provide a consolidated view of Civil Service data, optimised for reporting and analysis. It, therefore, serves as a sustainable common source of information. In particular, this database contains selective transactions and inter-related information from all Government Information Systems, specifically structured for dynamic queries and analytics. In addition, these data is further analysed by special Decision Support Systems, providing the Government executives with a global view of the Civil Service operation and the facility to effectively monitor the tendencies to various matters, to derive useful conclusions and take quick decisions, based on accurate and reliable information.

To summarise, the GDW is a single database of consolidated Civil Service data, which enables easy access to accurate and integrated data. Public authorities are requested to apply to the Department of Information Technology Services (under the Ministry of Finance), for access. The Information Department is responsible, inter alia, for evaluating access applications to the GDW. The GDW could fall under the (shared) databases category as defined in Book VI, since it confers direct information access to the participating public authorities. Unlike the definition of “Database” under Chapter 1, Article V1-2 of Book VI, access is granted upon request after the necessary permit is acquired. For more information please see Answer to Question 2 below. Additionally, the GDW could also fall into the category of a structured information mechanism as defined in Book VI, since it allows all Government Departments with access to the repository to interact with each other by posing questions and receiving answers in the form of data.

In order to exemplify, the GDW can give access for example, to the national Information System of the Department of Land and Surveys of the Ministry of Interior, namely the Land Information System (“LIS”) database. This particular system centralises the following categories of data: survey, land, topography, land registration and valuation. In essence, the system operates four databases into one, single corporate database ((a) the Survey Database, (b) the Digital Cadastral Database, (c) the Topographical Database, and (d) the Legal/Fiscal Database). The Survey Database, the

Digital Cadastral Database and the Topographical Database constitute the spatial component of the LIS, and the Legal/Fiscal database mainly constitutes the aspatial component. Similarly, this system could also be classified into the category of a structured information mechanism and/or a shared database as defined in Article VI-2 of the ReNEUAL Model Rules, since it permits communication and interaction between public authorities in the conduction of their administrative tasks.

In this framework, all Government Information Systems can become shared databases, through the GDW and after permission is granted.

Similarly, at EU level, the INSPIRE Geo-Portal created by the European INSPIRE Directive (2007/2/EC) establishes a European Union (EU) spatial data infrastructure. This enables the sharing of spatial information among public sector organisations and better facilitate public access to spatial information across Europe. INSPIRE is based on the infrastructures for spatial information that are created by the Member States and which are made compatible with common implementing rules and are supplemented with measures at Community level. These measures ensure that the infrastructures for spatial information created by the Member States are compatible and usable in a Community and cross-border context. Network services are necessary for sharing spatial data between the various levels of public authority in the Community. These network services, such as the INSPIRE Geo-Portal of Cyprus make it possible to discover, transform, view and download spatial data and to invoke spatial data and e-commerce services according to the INSPIRE Directive.

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.**

Not long ago and certainly before the *GDPR* came into force, the now repealed Act *138(I)/2001* on Data Protection, made provisions for the connection of archives (shared databases, workflows and/or files) between public authorities, provided the necessary leave (permit) had been granted, under the provisions of the repealed Act and subject to certain statutory conditions being met. Such permits were issued by the Office of the Commissioner for the Protection of Personal Data. This statutory

arrangement is no longer available to public authorities since the Act has been repealed as of the 31/7/2018 and all issued permits have no legal effect as of the 24/5/2018.

Currently, all connections/accesses are permissible via the Government Data Warehouse ("GDW"), as explained above. As it has been explained, the objective of the GDW is to serve as a central repository of data and enable easy access to accurate, consistent and integrated government data for better and faster decision-making and for statistical purposes. It provides a single cohesive database of the Civil Service's consolidated data, optimised for reporting and analysis. In particular, this database contains selective transactions and inter-related information from all Government Information Systems, specifically structured for dynamic queries and analytics.

Public authorities are directed to the Department of Information Technology Services (under the Ministry of Finance), for the necessary permit to the GDW, which provides a national and secure information exchange environment. A circular of the Department of Information Technology Services, was disseminated to all public authorities in March 2018, informing them that, for any present or future needs of accessing the repository, public authorities should apply promptly to that effect.

In the event that an application for access to the GDW is rejected or the information system of a particular public authority access to which is requested by another public authority, does not participate in the GDW, then a pubic authority can apply to the Commissioner for the Protection of Personal Data for connections in accordance with the *Personal Data Protection against Processing and the Unobstructed Circulation of such Data Act of 2018, L.125(I)/2018* which has been enacted on 31st of July, 2018[1]. The statute provides for the connection of large-scale national information systems of public authorities. Specifically, section 10(1) of the statute provides that two or more large-scale systems can be connected/combined on public interest grounds and only if the conditions set out in Article 6(1)(c) or (e) or Article 9(2)(f), (g) or (h) of the *GDPR* are met. Terms and conditions may be imposed by the Commissioner as stipulated by section 10(4).

[1] The repealed statute L.138(I)/2001, has been succeeded by the new piece of legislation, L.125(I)/2018.

Moreover, under the *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, Detection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019*, the large scale information systems of two or more competent authorities (the Cyprus Police, Customs, the Unit for Combating Money Laundering and the Tax Department) or the systems of all of them or the system(s) of one or more of those competent authorities with other public authorities may be connected on public interest grounds and if the conditions set by the statute are met (section 31). Under section 31(4) of the same statute, the Commissioner for the Protection of Personal Data is responsible for granting the required permit and may also impose such terms and conditions as it deems fit.

Lastly, a more conventional mechanism of information exchange amongst public authorities is made available by virtue of section 45(2) of the *General Principles of Administrative Law Act of 1999*. Under section 45(2) a public authority is legally obliged to conduct a due enquiry into all the relevant facts of the case, before reaching its final decision and while exercising its discretionary powers. In accordance with the provisions of the section, the enquiry may be conducted by the public authority itself or through another authority or person. It, therefore, allows for the exchange of information between public authorities when the required enquiry is undertaken. However, since this information exchange is initiated upon request, in individual cases, in situations where the requesting authority asks for support in fulfilling its administrative obligation for a thorough enquiry and the information gathered is done in accordance with the needs of the requesting public authority, it can safely be said that, this provision, largely falls within the framework of informational mutual assistance and not within 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?

Generally speaking, an impact assessment must always be conducted during the initial stages of policy-making and in any case before any decision for statutory intervention/amendment is taken.

More specifically, it is compulsory to file an Impact Assessment Report with every new Bill, proposed Regulation, Order and Directions (primary and subsidiary legislation) which might significantly affect the private and/or public sector and/or the citizens. Impact Assessments mainly focus on the impact the new piece of legislation will have on the economy, society and the environment. A comprehensive Guide to Impact Assessment was made available by the Unit of Administrative Reform of the Presidency of the Republic of Cyprus which sets out clear guidelines in relation to the subject-matter.

Considering that such advance forms/systems of information exchange are usually established and regulated by law or by Decision of the Council of Ministers and generally speaking, they may potentially have an impact, on, inter alia, the public sector, the economy and society, an impact assessment (and pertinent consultations) would need to be conducted before securing their establishment.

Furthermore, with respect to personal data and by virtue of section 13 of the national legislation on *Personal Data Protection against Processing and the Unobstructed Circulation of such Data Act of 2018, L.125(I)/2018*, an impact assessment (as well as consultations conducted with the Commissioner) is required before a new law or Regulation, on personal data processing, is enacted; unless a satisfactory impact assessment has already been conducted for another piece of legislation and the Commissioner is of the opinion that an additional impact assessment is not required.

By virtue of section 10(2) of *L.125(I)/2018*, an impact assessment (as well as consultations with the Commissioner) is also required when two or more large scale information systems of public authorities are connected and they concern sensitive personal data (race, political beliefs, religion, sexual orientation, past convictions etc) or the connection will be conducted by the use of citizens' personal identification number or any other identification element. This particular impact assessment must include all the information required by Article 35(7) of the *GDPR* and a description of all technical and organisation measures as provided by Articles 24, 25, 28 and 32 of the *GDPR*.

Similarly, and also with respect to personal data, a Data Protection Impact Assessment (DPIA) is required under Article 35 of the *GDPR* every time a controller begins

a new project that is likely to involve “a high risk” to other people’s personal information. According to Article 35:
“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data”.

Identical provisions are made under section 28 of the *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, Detection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019*. The impact assessment must include a description of the processing undertaken, an assessment of the risk this will have on the rights and freedoms of the data subjects, the measures that can be taken in light of these risks as well as all necessary security measures and mechanisms to be undertaken in order to safeguard the data and ensure compliance with the provisions of the statute.

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?

As far as administrative jurisdiction is concerned, the General Principles of Administrative Law Act of 1999, like the ReNEUAL Model Rules, encapsulates and safeguards the most fundamental principles of administrative justice. In 1999, the General Principles of Administrative Law codified the case law of the Supreme Court into a statute with the primary aim to safeguard administrative decision-making, by the provision of rules. Since 1999, technology has made giant leap steps forward in, inter alia, information exchange systems. The statute, although an indispensable pillar to administrative decision-making and administrative proceedings, does not, unlike the ReNEUAL Model Rules, establish general rules concerning advanced imformation exchange systems. The reality is that the growth and application of these systems was introduced into the public law sphere well before anyone could properly reflect on how these systems interrelate with the administrative law principles as enshrined

in the statute. In a nutshell, the statute incorporates the principles of fairness, competence, proper administration- bona fide and proportionality, legality, representation, due enquiry, natural justice- impartiality and right to be heard, equality, right to judicial review and to an appeal. Administrative decision-making is hence, rule-guided by the aforementioned principles. In addition, the said statute is applicable to all levels of administration in Cyprus; to the central government as well as to regional, local public authorities and semi-governmental organisations.

In this context, the following arguments can be made in relation to these mechanisms of advanced information systems, starting with the national legal framework:
Judicial review of administrative action is introduced as a separate jurisdiction by Article 146 of the Constitution of the Republic of Cyprus. It provides that the administrative jurisdiction of the Administrative Court and of the Supreme Court is exercised on decisions, acts or omissions of any organ, authority or person, exercising an executive or administrative authority, within the domain of public law. In that respect, only action or inaction of the administration productive of legal consequences can constitute the subject of review. This is important in the sense that only executory acts are amenable to judicial review. Executoriness connotes action expressive of the will of the public authority determinative in itself of the rights and obligations of the subject(s) of the decision.

In brief, for a decision to be amenable to judicial review within Cyprus' legal framework certain requisites must co-exist which are always assessed by the Court ex proprio motu and are as follows:

- The decision must have been taken by an organ, or authority or person exercising executive or administrative authority in the domain of public law.
- The executory nature of the administrative decision; that is an action expressive of the will of the administrative body.
- Judicial review may only be brought by an applicant who has an existing and direct legitimate interest in the matter.
- Strict time limitation conditions.

With these in mind, it would be fair to say that, information exchange does not constitute nor produce legally binding effects with regard to the person concerned. Even if the law requires utmost account to be taken of information provided by another public

authority it is only a preparatory step to the final decision. Acts of a preparatory nature of the administration are not susceptible to judicial review. Preparatory acts are those that prepare an executory administrative decision, as explained above, and are necessary or useful for its issuance. The final decision is, hence, the legally binding act.

Furthermore, Book VI of the ReNEUAL Model Rules which supplements Book V (and Book III), regulates advanced forms of inter-administrative information exchange which are central features of information exchange within the composite and multi-jurisdictional European administration. Limitations therefore, arise, from the very different context of a multi-level integrated administrative structure, such as the EU, by comparison to the situation within a unitary state. Hence, the reality of the composite, multi-jurisdictional decision making in the EU is very different to the national administrative procedure where administration is looked at as a unit.

In conclusion, in accordance with the doctrine of separation of state powers, it is a fundamental and settled principle of law that the judiciary does not step into the sphere of administration. The jurisdiction of the Court is delimited to the review of the legality of the act, decision or omission. When reviewing the legality of a decision, the Court examines whether the public organ has exercised its discretionary powers, within lawful limits, but its jurisdiction does not extend to issues of technical nature or issues that require specialised knowledge[2].

In order to briefly exemplify, the Court will only intervene if after taking into account all the facts of the case, it concludes that the findings of the administrative body are not reasonably sustainable, or they result from an error of fact or law or are in excess of its discretionary powers[3]. In essence, the court reviews the decision in order to ascertain whether:

- there is a clear statutory empowerment of discretion and its extent,
- the public body has exercised its discretionary powers correctly, without abuse and within the limits prescribed by the law, the Constitution and the general

[2] Storey v. Republic (2008) 3 C.L.R. 113, Republic v. C. Kassinos Constructions Ltd (1990) 3 (E) C.L.R. 3835, Lambrou v. Republic (2009) 3 C.L.R. 79, Georghiou v. SALA (2002) 3 C.L.R. 475, Eva Ttousouna v. Republic (2013) 3 C.L.R. 151

[3] Republic v. Georghiades (1972) 3 C.L.R. 594, Yuri Kolomoets v. Republic (1999) 4 A C.L.R. 443

principles of administrative law[4]. Therefore, the court reviews whether the public body has abused its discretionary powers or acted excessively or in an ill manner[5] and

- there has been sufficient enquiry of all relevant and material facts of the case and the administrative authority has evaluated and balanced all the facts of the case and no misconception as to the real and material facts of the case is manifested.

In light of this background, it is further stressed that the court's jurisdiction does not extend to issues of technical nature or issues that require specialised knowledge[6].

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 it-self?

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 *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, Detection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019* makes specific provisions on the matter. First, by virtue of section 5, the data processor must ensure that the personal data is correct. Incorrect data must be erased or corrected immediately. The processor must take every reasonable measure in order to ensure that inaccurate, insufficient data as well as data that are not up-to-data are not transmitted, shared nor exchanged (section 3). In accordance with section 9, incorrect data or data that are not up-to-date must never be exchanged/shared. Similarly, the processor is obliged to check, to the extent possible, the quality of the personal data before any exchange/sharing takes place. By virtue of the same provision, all necessary information must be given to the

[4] Action and Control of Administration, Nicos Chr. Charalambous, 2014, 2nd Edition, Page 315
[5] Cyprus Administrative Law Manual, Nicos Charalambous, 3rd edition, 2016, Page 304-305
[6] Storey v. Republic (2008) 3 C.L.R. 113, Republic v. C. Kassinos Constructions Ltd (1990) 3 (E) C.L.R. 3835, Lambrou v. Republic (2009) 3 C.L.R. 79, Georghiou v. SALA (2002) 3 C.L.R. 475, Eva Ttousouna v. Republic (2013) 3 C.L.R. 151

receiving authority in order to be able to establish and confirm the accuracy, the credibility (validity) of the data as well as the extent to which these data have been brought up-to-date. In accordance with the provisions of the statute, if inaccurate data have been exchanged the receiving authority must be informed immediately.

On a wider scope and within the framework of administrative jurisdiction the following points can be made:
As a rule, administrative decision-making is not subject to the agreement or consent of a third party. In this respect, a public authority acts, unilaterally, conferring rights or obligations upon persons. This unilateral expression determines the content of the decision. Although this is accurate, administrative decision-making is, on the other hand, subject to the sine qua non requirement of a thorough enquiry. Before a decision is reached, a public authority is under a legal obligation to conduct a due enquiry of all relevant facts, in accordance with section 45 of the *General Principles of Administrative Law Act of 1999, L. 158(I)/1999*.

Since administrative power involves as a rule, discretion in a manner that promotes the ends of the law, holding a due enquiry into the facts of the case is a prerequisite for a valid decision. The extent of the enquiry depends on each, individual case. Eliciting the material facts, as defined by the requisites of the law and the circumstances of the case, is of the essence. The means and the manner in which the enquiry will be conducted is a choice that lies with the public authority itself. Administration may also choose whether the enquiry will be conducted by the body itself or by or through another authority or person. As long as there has been a sufficient enquiry of all relevant facts for the discretion to have been exercised correctly, reasonably and under no misconception, the court will not intervene. In other words, the assessment of the facts lies with the administration and in so far as the evaluation made and the conclusions drawn therefrom are reasonably open to it, the Court will not intervene with a choice resting thereupon. Failure to conduct a due enquiry, on the other hand, could lead to misconception of facts materially affecting the decision made and result in its voidance.

Moreover, if discretion is vested in a public authority, the public authority is under a legal obligation to exercise it. Abstention, is an omission to act and would render the

decision void. Being substituted or directed by another public authority is also not permissible. Under the provisions of section 44(2) of the *General Principles of Administrative Law Act of 1999*, a public authority cannot be substituted or directed by another organ in the exercise of its discretionary powers.
Concluding from the above, all information/facts must be assessed by the competent public authority within the prism of a due enquiry and within the bounds of its discretionary powers, before a final decision is reached.

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?

Please see Response to Question 5a).

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?

A. With regard to the Government Data Warehouse ("GDW")- discussed in the Responses to Questions 1 and 2- the following observations can be made. As it was previously mentioned, the GDW is a single cohesive database with a subject-centric approach, in order to provide a consolidated view of Civil Service data, optimised for reporting and analysis. In particular, this database contains selective transactions and inter-related information from all Government Information Systems, specifically structured for dynamic queries and analytics. In other words, the GDW is fed with information and raw data from all Government Information Systems with the ability, inter alia, to perform dynamic queries. Hence, the system has been developed in such a way as to provide answers to Governance Questions- "GQs". For this purpose, the GDW draws information from the raw data that each Ministry/Department/Office has uploaded to the system. Safeguards are in place in order to make sure that personal data are protected. For example, when a GQ of a particular Ministry/Department/Office uses data fed into the system by another Minis-

try/Department/Office, the first must receive the consent of the latter. GQs can be performed in search of information for a particular citizen. Access to such a GQ is only granted to a restricted number of Officers within the Ministry/Department/Office. If a GQ aims at analysing behaviours or in profiling, the GQ cannot be used in the decision-making process in relation to that particular person.

B. Under the due enquiry requirement for a thorough examination of all relevant and material facts of the case, before a public authority reaches its decision and, in a situation, where the participating public authority, draws personal data from the GDW repository, then the principles as they have been explained in paragraph A. above apply.

C. If national information systems have been connected/combined under the provisions of the *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, Detection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019*, then the participating authorities will have unobstructed access to those data. Processing is only permissible in accordance with the purpose of the statute, otherwise if a different purpose is sought, the provisions of the *GDPR* apply. Special provisions apply for the processing of personal data of particular categories (namely factors such as race, political beliefs, religion, participation in organisations, genetic and biometric data, health, sexual orientation, sexual life and past convictions). Special provisions also apply if personal data will be transmitted to a third country or to an international organisation (Part V of the statute). Where personal data is made available by another Member State, prior approval for the transmission is required in accordance with that MS' national law (section 38(1)(c)); unless the transmission is necessary for the prevention of an immediate and serious threat to the public safety of the Republic or another MS' or to a third country's or in order to safeguard the substantial interests of another MS.

D. Moreover, if national information systems have been connected/combined under the provisions of the provisions of the *Personal Data Protection against Processing and the Unobstructed Circulation of such Data Act of 2018, L.125(I)/2018,* then the participating authorities will have unobstructed access to the data, unless terms and conditions have been imposed by the Commissioner in accordance with section 10(4) of the statute. Special provisions apply if personal data will be transmitted to a third country or to an international organization (section 18).

E. With regard to communication data and under Article 17.2 of the Constitution interference with the right to privacy is only permitted after a court order is issued for the investigation or prosecution of a serious criminal offence punishable with imprisonment of 5 years and over and the interference concerns communication data necessary to identify an individual user or to provide information about their online activity.

F. A rather different situation is stipulated under section 17(5) of the General Principles of Administrative Act of 1999, which does not necessarily concern information exchange systems. Under the provisions of section 17(5), if an application and/or information is submitted to a non-competent public authority, then an obligation arises for this body to convey it (all information including personal ones) to the competent public body, as soon as it establishes that it lacks competence. Under this situation, the non-competent public authority, must inform, the person concerned, straight away, that due to competence issues his application (information) is conveyed to the competent body for processing. Failure to do so, however, does not entitle the person concerned to an enforceable right to lodge a judicial review recourse before the Administrative Court. Nowadays, the Government Gateway Portal ‘Ariadne’ has stepped in to offer a solution. Ariadne enables citizens to use online electronic services (e-Services) of the Government of Cyprus. Citizens as well as public authorities need to register in order to have access to Ariadne.

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?

The protection of personal data of natural persons is a fundamental right enshrined in Article 8 of the *European Convention on Human Rights* (Right to respect for private and family life, home and correspondence), Article 16 of the *Treaty on the Functioning of the European Union* (Everyone has the right to the protection of personal data concerning them) and Article 15 of the *Constitution of the Republic of Cyprus*.

The *General Data Protection Regulation (GDPR)* provisions:

The *GDPR* gives individuals the right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller.

The law distinguishes between two cases: (a) where personal data is directly obtained from the data subject (Article 13 of the *GDPR*) and, (b) if this is not the case (Article 14 of the GDPR).

Where data is obtained directly, the person must be immediately informed, meaning at the time the data is obtained. In terms of content, the controller's obligation to inform includes his identity, the contact details of the Data Protection Officer (if available), the processing purposes and the legal basis, any legitimate interests pursued, the recipients when transmitting personal data, and any intention to transfer personal data to third countries. In addition, the right to be informed also includes information about the duration of storage, the rights of the data subject, the ability to withdraw consent, the right to lodge a complaint with the authorities and whether the provision of personal data is a statutory or contractual requirement. Moreover, the data subject must be informed of any automated decision-making activities, including profiling. Only if the data subject is already aware of the above information it is not necessary to inform and provide it.

If personal data is not obtained from the data subject, the person must be provided with the information within a reasonable period of time, and at the latest within a month. In cases where the gathered information is used to directly contact the data subject, he or he has the right to be informed immediately. As far as content is concerned, the controller has to provide the same specific information as if the personal

data were obtained directly from the data subject. In addition, the controller has the obligation to inform from what sources the personal data originated, and whether it was publicly available. The data subject has a right to be informed in a precise, transparent, comprehensible and easily accessible manner. The obligation to be informed can be fulfilled in writing or electronically. In exceptional cases there is no obligation to inform. This applies, where the provision of information is either impossible or unreasonably expensive, the gathering and/or transmission is required by law, or if the data must remain confidential due to professional secrecy or other statutory secrecy obligations.

If a person thinks that his or her personal data have not been respected, the person concerned may lodge a direct complaint before the Office of the Commissioner for Personal Data Protection alleging a personal data breach. The Office of the Commissioner is an Independent Supervisory Authority for the protection of the individual. Before doing so though, the data subject may contact the controller of the data directly or if a Data Protection Officer (DPO) has been appointed, he or she may contact the DPO, for exercising his or her rights (right of access, right to object or to rectification or to erasure or to restriction of processing or to data portability). In case of an established breach, the Commissioner may impose corrective measures (including fines etc) to controllers or processors. The Commissioner may also refer the case to the Police and notify the Attorney-General of the Republic if any violation of the *GDPR* or the national legislation *Act 125(I)/2018* constitutes an offence in accordance with the provisions of section 33 of the aforementioned national statute. The Commissioner's decision may be appealed before the Administrative Court and subsequently, the decision of the Administrative Court may be appealed before the Supreme Court.
A person may be entitled to compensation if he or she has suffered material damage, such as financial loss, or non-material damage, such as psychological distress. Compensation may be sought by bringing a claim before the Civil Courts. The Commissioner is not competent to grant any sort of compensation to aggrieved data subjects.

Likewise, similar provisions exist under the *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, De-*

tection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019. By virtue of section 15, the controller's obligation to inform includes his identity, the contact details of the Data Protection Officer (if available), the processing purposes and the legal basis, any legitimate interests pursued, the recipients when transmitting personal data, and any intention to transfer personal data to third countries. In addition, the right to be informed also includes information about the duration of storage, the rights of the data subject, the right to lodge a complaint with the authorities (Commissioner) and the legal basis for processing. These rights may be restricted, inter alia, for reasons of public security, national safety or for preventing the obstruction of investigations etc. Under section 48, if a person thinks that his personal data have not been respected, he may file a complaint to the Commissioner. The Commissioner's decision may be appealed before the Administrative Court and subsequently, the decision of the Administrative Court may be appealed before the Supreme Court. He may also bring a recourse before the Administrative Court, against the controller or the processor, alleging infringement of his rights as a result of the processing. A person may be entitled to compensation if he has suffered material damage, such as financial loss, or non-material damage, such as psychological distress. Compensation may be sought by bringing a claim before the Civil Courts (section 52 of the Act).

At EU level, information exchange systems operating on a large scale such as EUROPOL, SIS-II, EUROJUST, EURODAC, Internal Market Information System (IMI), Customs Information System (CIS) and Visa Information System (VIS) are supervised by the European Data Protection Supervisor and at national level, by the Commissioner for Personal Data Protection. The role of the Commissioner as the national supervisory authority, is to supervise the national systems, ensure that the competent authorities of the Republic process personal data in accordance with EU and national legislation and to make sure that citizen's rights are exercised in line with these legislations. All aforementioned large scale Information Systems, operating in the EU, contain certain rights for the data subject. The SIS-II Regulation, includes, inter alia, the right to be informed if there is an alert issued against the data subject. The information must be in writing and be accompanied with a copy or a reference to the national decision issuing the alert. The rights can be restricted by national law, for reasons such as safeguarding national security or for the prevention of criminal of-

fences (amongst others). Furthermore, by virtue of section 13 of the national statute for the *Establishment and Functioning of the National Europol Unit of 2018, L. 126(I)/2018*, a person has the right to be informed (exercised upon request), if Europol is processing his/her personal 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.

While the legal consequences of a legally binding decision can be formally quashed by a court, information has a mainly factual impact which is much more complex. In the event that information entered into the system is false and the falsity of it has materially affected the decision taken, then the following can be said to apply.
Starting from the legal framework, it should be borne in mind that judicial review in Cyprus is not exclusively restricted to grounds of legality only. It is extended upon several grounds including factual questions and circumstances. Briefly, the court reviews grounds such as misconception of fact and law, lack of due reasoning/justification, absence of sufficient enquiry and abuse of power. The assessment of the facts lies with the administrative authorities and in so far as the evaluation made and the conclusions drawn therefrom are reasonably open to them and the public authorities acted within the parameters of the law, they are the sole arbiters of their decisions and the Courts will not interfere with a choice resting thereupon. Misconception of facts, on the other hand, materially affecting the decision made will result in its voidance[7] and the burden of proof is borne by the Applicant[8]. An administrative authority may not take into account irrelevant or non-existent facts or fail to take into

[7] Papantoniou and others v. Public Service Commission (1983) 3 C.L.R 64
[8] Platritis v Republic (1969) 3 C.L.R. 366, Papadopoulos v. Tax Department (1990) 3 C.L.R. 262, 267

account substantial / material facts to the case. However, as long as the public authority has evaluated and balanced all material facts of the case, even contradictory ones, it may give greater weight to some than others, if such a choice is within the bounds of reason. With this in mind, if false information has materially affected the decision taken, then the court will declare that decision void. If, on the other hand, this information entered into the system, which ultimately turned out to be false, has not penetrated or materially affected the decision then no misconception of facts will be found by the court.

In practice, it is often the case that, once an administrative authority becomes aware of the fact that relevant information/facts taken into account at the decision-making stage, are ultimately false or non-existent and those facts have materially affected the decision taken by it, the public authority, shall proceed to revoke the decision and a new decision is thereafter issued. Proceedings are not terminated if the revoked act, caused material damage to the applicant which can only be claimed once the administrative decision is annulled.

In the occasion that an information system malfunctioned the following observations can be made:
First, both the Administrative Court and the Supreme Court, in its judicial review jurisdiction, when reviewing the legality of a decision, examine whether the public authority has exercised its discretionary powers, within lawful limits. Their jurisdiction, though, does not extend to issues of technical nature or issues that require specialised knowledge[9].

However, if a due enquiry is hindered by a system malfunction, then the public authority duty-bound to conduct a due enquiry, is under an obligation to conduct such enquiry into all the material facts of the case, aided by other, alternative means. If due to the malfunctioning the competent public authority was unable to conduct a due enquiry into all the relevant facts of the case and at the same time it has failed to conduct an enquiry through alternative means and the Court held that the decision

[9] Storey v. Republic (2008) 3 C.L.R. 113, Republic v. C. Kassinos Constructions Ltd (1990) 3 (E) C.L.R. 3835, Lambrou v. Republic (2009) 3 C.L.R. 79, Georghiou v. SALA (2002) 3 C.L.R. 475, Eva Ttousouna v. Republic (2013) 3 C.L.R. 151

reached is a product of an incomplete, insufficient or non-diligent enquiry, materially affecting the decision reached, then, the decision will be declared void by the Court.

Holding a due enquiry into the facts of the case is a sine qua non prerequisite for a valid decision of a public authority. The extent of the enquiry depends on each, individual case. Eliciting the material facts, as defined by the requisites of the law and the circumstances of the case, is essential. The public authority is at liberty to choose the method with which the enquiry will be conducted. Failure to conduct a due enquiry could lead to misconception of facts (please see above for 'misconception of facts') rendering the decision void.

In any case, the jurisdiction of the court only goes so far as to annul the decision. The Administrative Court and the Supreme Court, in its judicial review jurisdiction, will not grant damages to an applicant who has suffered damages on account of an annulled decision. Damages may be ordered by a Civil court as explained further down. By virtue of Article 146.4 of the Constitution the Administrative Court may only:

- Confirm, either in whole or in part, the decision, act or omission; or
- Declare, either in whole or in part, the decision or act to be null and void and of no effect whatsoever; or
- Declare that the omission, either in whole or in part, ought not to have been made and that whatever has been omitted should have been performed; or
- Amend, either in whole or in part, the decision or act, subject to the provisions of the law, and provided that the decision or act concerns tax matters or international asylum procedures under European Union law.

Judgments of the Administrative Court may be appealed to the Supreme Court on points of law only.

Judgments issued are final and will acquire the force of res judicata[10]. A decision of the Administrative Court, or if an appeal has been filed the decision on the appeal, applies erga omnes; it binds all, both the applicant and the administrative body. The

[10] Section 59 of the General Principles of Administrative Law, Law of 1999

administrative body, however, is duty-bound with an extra obligation; to give effect to the court's decision, i.e. re-examine its decision bound by the judgment's dictum[11].

On the topic of damages, if the aggrieved person has suffered damages on account of an annulled decision, then, by virtue of Article 146.6 of the Constitution, he or she may seek compensation or another remedy and recover just and equitable damages to be assessed by a Civil Court or to be granted such other equitable remedy as the Civil Court is empowered to grant. In civil proceedings, judicial decisions are as a rule binding upon the parties and matters resolved thereby are treated as res judicata between them. Only decisions bearing on the personal status of a party, such as decisions affecting the birth, death and marital status, bind the world at large[12].

Under the *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, Detection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019*, the data subject has the right to request the correction of false personal data that concern him/her (section 18). More so, if his/her right has not been respected he may bring a recourse before the Administrative Court against the controller or the processor (section 50) and if material or non-material damages has incurred, he or she may claim compensation against the controller or against **another public authority** (Cyprus Police, Customs, Unit for Combating Money Laundering and the Tax Department) in accordance with the relevant law (section 52). In addition, the Commissioner can impose administrative sanctions on the competent authority acting as the processor (section 54).

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?

With regard to personal data, a data subject has the right of access, rectification, erasure and restriction of the data that concern him/her as provided by Articles 16,17

[11] Article 146.5 of the Constitution and sections 57 and 58 of the General Principles of Administrative Law, Law of 1999
[12] Nicolaides v. Yerolemi (1984) 1 C.L.R. 742 (CA)

and 18 of the *GDPR EU Regulation 2016/679* and section 18 of the *Protection of Personal Data against Processing from Competent Authorities for the Purpose of Prevention, Investigation, Detection or Persecution of Criminal Offences or the Execution of Criminal Sanctions for the Unobstructed Circulation of such Data Act of 2019, L.44(I)/2019*. The exercise of these rights may be subject to restrictions as EU and national legislation provides or as permitted by the national Commissioner for Personal Data Protection. If a person believes that his/her personal data have not been respected, he/she may lodge a direct complaint before the Office of the Commissioner for Personal Data Protection alleging a personal data breach (Article 77(1) of the *GDPR* and section 48(1) of *L.44(I)/2019*). The Office of the Commissioner is an Independent Supervisory Authority for the protection of the individual. Before doing so, the data subject may contact the controller directly or if a Data Protection Officer (DPO) has been appointed, he or she may contact the DPO, for any concerns and exercise of rights (right of access, right to object or to rectification or to erasure or to restriction of processing or to data portability). In case of breach, the Commissioner may impose corrective measures (including fines etc) to controllers or processors. The Commissioner may also refer the case to the Police and notify the Attorney-General of the Republic if any violation of the GDPR or of the national legislation *L. 125(I)/2018* and L. 44(I)/2019 constitutes an offence in accordance with the provisions of section 33 and 55 of the aforementioned national statutes, respectively. The Commissioner's decision may be appealed before the Administrative Court and subsequently, the decision of the Administrative Court may be appealed before the Supreme Court. A person may be entitled to compensation if he/she suffered material damage, such as financial loss, or non-material damage, such as psychological distress. Compensation may be sought by bringing a claim before the Civil Courts. The Commissioner is not competent to grant any sort of compensation to aggrieved data subjects.

If a recourse is lodged before the Administrative Court under *Article 146 of the Constitution*, the Court has jurisdiction to review on both points of fact and law and is not bound by the findings of the administrative body as to the facts of the case. It may, therefore, take an independent view on the facts. However, the Administrative Court cannot substitute its own decision for that of the public body. This can only be done where the decision relates to matters of asylum and tax discrepancies, in accordance

with the provisions of the *Administrative Court's Act L. 131/2015*. In all other matters, it can only annul the decision on several grounds. Judgments of the Administrative Court can be appealed to the Supreme Court, on points of law alone.

Judicial review is intended to scrutinise the legality of acts or omissions and not to evaluate their correctness from the point of view of the judiciary. The correctness of the decision from the subjective viewpoint of the Court is not at issue except, to the extent that the choice made defies reason. By virtue of *Article 146.1. of the Constitution*, a justiciable act, decision or omission will be declared void if it is contrary to any of the provisions of the Constitution or of any law or is made in excess or in abuse of powers vested in such organ or authority or person. Therefore, if an aggrieved individual, disputes the correctness of a decision then, the right course of action is for the individual to bring a claim to a civil court and seek redress accordingly. If on the other hand, he/she disputes the legality of the decision the individual may bring a recourse to the Administrative Court. Amongst other things, the court reviews the decision in order to ascertain whether there has been sufficient enquiry of all relevant facts for the discretion to have been exercised correctly, reasonably and under no misconception. Misconception of facts materially affecting the decision will result in the voidance of the decision. False information that has materially affected the final decision taken by the public body will render the decision void. For a more elaborate explanation on this please see Response to Question 7 above for misconception of facts.

Moreover, if the aggrieved person has suffered damages on account of an annulled decision, then, by virtue of Article 146.6 of the Constitution, he/she may seek compensation or another remedy and recover just and equitable damages to be assessed by a Civil Court or to be granted such other equitable remedy as the Civil Court is empowered to grant.

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?

Administrative jurisdiction

National courts review final decisions and omissions of public authorities from their own nation. Indeed, situations may arise where the court reviews a final decision of a public authority from its own jurisdiction which was based on information exchange from another Member State or the final decision is based on a combination of information from various jurisdictions (multijurisdictional nature of information exchange). In this respect, authorities cooperate in the common interest, in a non-hierarchical manner and based on mutual trust. However, problems may arise when the national court reviewing the final decision of a public authority from its own jurisdiction, may also review factual input (information), based on information exchange from another Member State. In integrated forms of information exchange, it may be difficult to identify the source of information or the final decision may be based on a combination of information from various sources and jurisdictions. Similarly, problems may arise with regard to the review standards, for example concerning the applicable procedural standards for information gathering by a foreign country or duplication of procedures with potentially contradictory judgments.

Other jurisdictions (civil and criminal)

With respect to the arrest of requested persons between EU member States, the procedure is governed by the *European Arrest Warrant (EAW) and Surrender Procedures of Requested Persons between Member States Act of 2004, L. 133(I)/2004* (and the Framework Decision 2002/584/JHA). In the Member States where the Schengen Information System (SIS) is in operation (Cyprus does not yet use the SIS) the national SIRENE Bureaux plays an important role in the EAW process when a corresponding alert has been created in the SIS. The rules and procedures for Member States' cooperation concerning alerts for arrest based on EAWs are set out in Articles 24 to 31 of Council Decision 2007/533/JHA of 12 June 2007 on the estab-

lishment, operation and use of the second generation Schengen Information System (SIS II)10 ('SIS II Decision') and Point 3 of the SIRENE Manual11. Where transmission to Cyprus is required, the EAW can be sent either directly or by the relevant Interpol National Office. Transmitting via Interpol is provided for in Article 10(3) of the Framework Decision on EAW.
The central authority for issuing and executing EAWs is the Ministry of Justice and Public Order. The Cyprus Police, the Law Office of the Republic and Judges of the District Courts are key actors. Once a EAW is issued, the Interpol Office as well as the central authority will transmit it to the receiving autjority. To avoid duplicitous warrants, a centralised database exists called the STOP-LIST. Since Cyprus is currently under evaluation for integration into the Second-Generation Schengen Information System II (SIS II) (further details are given in the Response to Question II.2. below) the STOP-LIST centralised database is being coordinated/transferred to the Cyprus SIRENE Bureaux.

It may also be the case, that non-nationals are requested to be extradited to their country of origin, if Contracting Agreements are present that bind bilaterally or multilaterally the contracting parties to this effect. The procedure for extraditing fugitives is laid down in the respective bilateral agreement and the *European Convention on Extradition* of the Council of Europe which was ratified into national law with the enactment of *L.97/1970* and three of its Additional Protocols (L.23/1979 (Additional Protocol), L. 17/1984 (Second Additional Protocol).

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.

Cyprus is a signatory to the Convention implementing the Schengen Agreement but enjoys a temporary derogation under its Act of Accession of 2003 and although obliged to join, it is not yet part of the Schengen Area due to its territorial division. Cyprus participates and has been carrying out preparatory activities to integrate into the Second-Generation Schengen Information System II (SIS II) but is not yet connected to it.

The Cyprus SIRENE Bureaux has been established since 2005, under the European Union and International Police Cooperation Directorate of Cyprus Police. A number of law enforcement officers have been trained and all technical infrastructure for full integration into the SIS-II has been implemented and are ready for operation (N-SIS, C-NIS as well as the communication infrastructure between the central system and the national system).

As a matter of fact, the Republic of Cyprus has submitted an application to join the Schengen Area in the summer of 2019, it is currently under evaluation and provided it receives a positive assessment on all required fields it will become a participating member State to the Schengen area.

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.

The legal arrangement of substitutional liability or subrogation mechanism that exists only for the SIS-II, under which any Member State is directly liable to a damaged person must be assessed in light of the Response to Question II.2 above. Under this arrangement if the state against which an action is brought is not the state issuing the Schengen alert, the latter shall be required to reimburse, at the request of the State sued. The sums must be paid as compensation unless the data were used by the requesting state in breach of the Convention. Since Cyprus enjoys a temporary derogation, it is currently under evaluation and is not yet connected to SIS-II, the legal arrangement of substitutional liability will apply to it as soon as it becomes a full member of the Schengen Area.

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).

Not as far as it is known.

Mr. Justice Leonidas Parparinos
Supreme Court of Cyprus