Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Netherlands

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 of The Netherlands

Introduction:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The General Administrative Law Act (GALA) does not contain any specific provision regarding the information exchange among authorities. The same goes for the Freedom of Information Act (*Wet openbaarheid van bestuur*), which is written mainly to oblige government bodies to disclose information to civilians, but not among authorities. There are however some other specific provisions.

Databases

With regard to the category 'databases' as defined in Article VI-2 (3) of the Re-NEUAL Model Rules, reference may be made to the System of Basic Registrations (*Stelsel van basisregistraties*). Public authorities should make compulsory use of the data from the Basic Registration System when performing their public tasks. There are currently ten basic registrations, relating to persons (*Basisregistratie personen*), trade (*Handelsregister*), addresses and buildings (*Basisregistratie adressen en gebouwen*), Land Registry (*Basisregistratie Kadaster*), Topography (*Basisregistratie topografie*), Large Topography

(*Basisregistratie grootschalige topografie*), Substrate (*Basisregistratie ondergrond*), vehicles (*Basisregistratie Voertuigen*), income (*Basisregistratie Inkomen*) and Immovable Affairs (*Basisregistratie Onroerende Zaken*). They have in common that they all must meet a dozen requirements (system characteristics), including a duty to use the basic registrations in its decision-making without further investigation. The different holders of basic registrations and the recipients of information have a joint responsibility for the accuracy and completeness of the information contained in the registration.

As the use is mandatory, strict quality requirements apply to the basic registrations. A parliamentary letter of 2003 mentions twelve quality requirements. For example, each basic registration must have a formal legal basis. Also, the user of the data from the basic registration (a public authority) is allowed to use the data without the need to conduct any further research regarding the authenticity of the information.[1] It is therefore not required for the user to carry out independent verification of the accuracy of the data. The letter explicitly states that this does not mean that existing procedures for determining the accuracy of the data have ceased to exist.[2] There may indeed be additional procedures. Although, in principle, the reliability and accuracy of the data can be assumed, this does not mean that the registrations are error-free. The broad use of the data does reveal errors sooner, thus revealing a so-called 'self-cleaning effect', according to the letter of Parliament.[3] In addition, the user of the registration has a duty to report to the holder of the basic registration if the accuracy of the information is in doubt.[4] The holder must then examine the notification and make corrections. If the information contained in the register is taken from another register, the notification must also be sent to the holder of the original register. Users can make feedback on the data contained in the Basic Registration Persons by using the Feedback Provision (*terugmeldvoorziening*).[5]

An example is the Basic Register of Persons (BRP). Municipalities include personal data of citizens (residents) in the BRP. When a person marries, gets a child or moves, this will be registered. When someone moves to another municipality, these personal data will be open for other public authorities to use for their acts relating to this person. The Minister of Interior and Kingdom Relations may then, at the request of an eligible organisation (who files 'an authorisation application'), adopt an 'authorisation decision' for the systematic provision of data from the Basic Registration Persons.

Other forms of information exchange

Apart from the databases as described above, partnerships (or cooperations) have been established between public authorities and private organisations (*samenwerkingsverbanden).* These partnerships do not have a formal legal basis but are based on convenants and protocols (see answer to question two).

---

[1] See requirement No. 1.1 from the letter of parliament, 2002/03, 26 387, No. 18, p. 12.
[2] Letter of parliament 2002/03, 26 387, No. 18, p. 13.
[3] Letter of parliament 2002/03, 26 387, No. 18, p. 13.
[4] Letter of parliament 2002/03, 26 387, No. 18, p. 12-13.
[5] See https://www.rvig.nl/brp/het-melden-van-vermoedelijke-fouten-in-persoonsgegevens.

General Data Protection Regulation (GDPR)

It must be noted that the requirements stemming from the General Data Protection Regulation (GDPR and the Implementing Law (*Uitvoeringswet Algemene Verordening Gegevensbescherming*) apply to the processing of personal data in the System of Basic Registrations by public authorities. Sector-specific laws (e.g. the Police Data Act and the Law on Judicial and Criminal Data) (*Wet politiegegevens* and the *Wet justitiële en strafvorderlijke gegevens)* contain additional requirements that need to be fulfilled before the exchange of data between public authorities (and private organisations) can take place. An example of a sector-specific law containing additional requirements for data exchange, is the Act on the exchange of information on above ground and underground nets and networks (*Wet informatie-uitwisseling ondergrondse en bovengrondse netten en netwerken).* The act sets out requirements for storing and sharing data concerning the geographical location of cable networks. Another example is the Passport Act (*Paspoortwet)* which provides for a register for travel documents. The data stored in this register can be shared with institutions in so far as necessary for the performance of a public task.

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.

Partnerships between public authorities

In addition to the categories of public information management as set out in Article VI-2 of ReNEUAL, the Netherlands has partnerships (*samenwerkingsverbanden)*. These partnerships have no formal legal basis but are based on covenants and protocols. The covenants and protocols reflect the relevant (legal) tasks of the parties involved. The partnerships do not have decision-making powers as such.[6]

As mentioned above, the partnerships are collectives of public authorities and/or private parties which jointly process data for important public interests. Some partnerships focus speci-fically on combating fraud and organized crime.[7] Other partnerships have a broader remit, as some examples will show:

The first example is '*Suwinet-Inkijk'. Suwinet-Inkijk* offers public authorities and private organisations the possibility to consult personal data from citizens stored by other public authorities or in the Basic Registrations as mentioned above. Municipalities as well as implementing authorities use *Suwinet-Inkijk* when performing their public tasks. The tasks of the involved parties are defined in the Work and Income Structure Act (*Wet structuur uitvoerings-organisatie werk en inkomen*).

[6] Report of the Working Group on the Data sharing Framework law 2014, p. 17.

[7] Report of the Working Group on the Data Sharing Framework Law, *Knowledge is power: Towards a better and more rigorous data exchange in partnerships,* The Hague, 5 December 2014, p. 15-17.

Other partnerships are the Financial Expertise Centre (*FEC*), which focuses on strengthening the integrity of the financial sector, and the Regional Information and Expertise Centres (*RIECs*), which collect and analyse signals on criminal activities (e.g. skimming, phishing and whitewashing). The Tax Department, the Public Prosecution Department (*het OM)*, the National Police and the Authority Financial Markets (*AFM*) are part of the Financial Expertise Centre. Rules on the exchange of data in the 'FECs' are defined in a covenant and an information protocol.[8] Rules on data exchange in the 'RIECs' are defined in an administrative agreement and a covenant.[9]

As indicated earlier, a number of partnerships have been established specifically to combat organized crime. Reference can be made to the regional 'cannabis agreements'. These partnerships include local governments, housing corporations, the National Police and the Public Prosecutor Department. Another example is the National Skimmingpoint partnership, which deals with combating fraud by skimming. Among others, the Minister for Security and Justice, the National Police, the Public Prosecution Department and the Paying Association (*betaalvereniging)* are members of this partnership.

Processing of personal data

When exchanging personal data within a partnership, the purpose for which the data is disclosed must be compatible with the purpose for which the data was originally collected (i.e. to fulfil a specific legal task). The rules governing the processing of data are of a 'vertical' nature; the data exchange occurs within a given sector. Partnerships, on the other hand, have a 'horizontal' character; the exchange of information appears between different sectors. In so far as sector-specific rules provides for criteria for this type of information exchange, the rules only apply to the situation that there is an exchange of information between two parties, not several at the same time. It must also be noted that if there are no sector-specific rules for the exchange of personal data between authorities, consideration should be given to the requirements as set out in the GDPR. Public authorities exchanging data in partnerships must always act in compliance with the GDPR. Public authorities find it rather difficult to examine whether the exchange of personal data is in line with the GDPR. For this reason, a legislative proposal which regulates the exchange of personal data within partnerships (*Wetsvoorstel gegevensuitwisseling samenwerkingsverbanden*), is pending.

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?

The exchange of data between governing bodies is laid down in more detail in many laws, but a default impact assessment is not prescribed. Some practical approaches have been developed, however. One example is the exchange of data for organisations working in the

[8] Covenant FEC 2009, Dutch Government Gazette 2009, 71 and Information Protocol FEC 2011, Dutch Government Gazette 2011, 21708.
[9] See Report of the Working Group on the Data Sharing Framework Law 2014, p. 16.

criminal justice chain (*strafrechtketen*), such as the police, the prosecution department, courts etc. This gives the following instructions to the organisations concerned:

1. Identify the process and the points at which professionals (organisations) share data.
2. Assess whether the data may be shared (lawfulness).
3. Assess whether there are risks if these data are shared.
4. Describe (planned) measures to control the risks.

Once all steps have been taken, an organisation complies with the obligation to produce an impact assessment (*PIA*). A PIA helps where personal data are processed and shared in order to identify and assess the impacts for data subjects.[10]

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?

Very little case law exists on the exchange of information between public authorities (within partnerships). However, a judgement of de district court of Overijssel from last year is worth mentioning. The court ruled that, in the view of Article 8 of the Dutch law on the Protection of Personal Data (now replaced by the GDPR), the exchange of personal data by public authorities must always have a formal legal basis and should be in conformity with the principles of proportionality and subsidiarity. The court dismissed the unsubstantiated position of the public authority that the processing of the personal data was necessary for the proper performance of a public task. Since there was (i) no legal basis to exchange the data, (ii) the data subject had not consented to the transfer of his personal data and (iii) the principles of proportionality and subsidiarity were violated, the court dismissed the appeal of the public authority.[11]

Case law with regard to the System of Basic Registrations usually concerns requests from citizens to view or correct their personal data stored in the Basic Registrations. The Council of State has ruled several times that data stored in Basic Registration should be as reliable and clear as possible and users should be able to rely on the accuracy of the data.[12]

In a last judgement worth mentioning, the Association of Dutch Municipalities (VNG) had set up a forum to enable its members to exchange information. The court ruled that although the VNG had the control, the members themselves were responsible for the data they placed on the forum. The forum was only used to exchange practises on a certain topic; there was no internal consultation. However, when processing personal data, public authorities must always act in compliance with the relevant provisions of data protection laws (currently the

[10] https://www.strafrechtketen.nl/onderwerpen/gegevensuitwisseling-tussen-organisaties
[11] District Court of Overijssel 18 July 2018, ECLI:NL:RBO:2018:2496.
[12] Council of State 23 May 2018. ECLI:NL:RVS:2018:1673, Council of State 11 January 2017, ECLI:NL:RVS:2017:22 and Council of State 18 maart 2015, ECLI:NL:RVS:2015:866.

GDPR). This judgement makes clear that public authorities can also cooperate in a more (informal) way.[13]

One ongoing court proceeding is the court case which the Platform Protection Civil Rights started against SyRi (System Risk Indication or *Systeem Risico Indicatie*). SyRi is a system which allows government to combat fraud in social matters. The tool allows central and local government authorities to combine broad categories of data previously stored separately, analyse them using an undisclosed "risk model", and identify some people as more likely to commit benefit fraud. Since its introduction, it has been used exclusively in areas with a high proportion of low-income residents, migrants and ethnic minorities. The basis for SyRi is a law which aims at 'comprehensive public intervention with regard to preventing and combating unlawful use of public funds and public services in the field of social security and income-related schemes, preventing and combating tax and contributory fraud and failure to comply with labour laws'. In order to reach this goal, SyRi makes it possible to link fifteen big data schemes which contain mass amounts of personal data of municipalities, the Tax Service, the Employee Insurance Agency et cetera. UN rights expert Philip Alston has stated that SyRi discriminates against the poorest members of society and undermines the rights to privacy and social security. Alston has made his analysis available to the court, emphasising in particular the disproportionate impact on the human rights of the poorest.[14] In a judgment of February 5th, 2020, the District Court of The Hague has stated that SyRi in its current form does not pass the test of Article 8 (2) ECHR.[15] The court has set the objectives of the SyRI legislation, namely preventing and combating fraud in the interests of economic well-being, against the breach of privacy. According to the court, the legislation does not comply with the 'fair balance' required by the ECHR for a sufficiently justified infringement of private life. The legislation is not sufficiently clear and verifiable as regards the deployment of SyRI. The legislation is unlawful because it is contrary to higher law and thus non-binding.

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?

See answer to question 1.

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.

[13] District Court of Rotterdam 4 June 2018, ECLI:NL:RBROT:2018:4317.
[14] https://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25152&LangID=E
[15] District Court of The Hague, 5 February 2020, ECLI:NL:RBDHA:2020:865.

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?

Not applicable; see question 1.

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?

The general rights of the data subject are formulated in the articles 12 and further of the GDPR. In line with the GDPR, Dutch legislation offers the data subject a right of access, to rectification, to reassure or the right to be forgotten et cetera. Dutch legislation does not provide for the automatic notification of the data subject when his or her (police) data are processed or exchanged.[16]

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

A citizen may submit a request to a public authority to grant access to his or her personal data stored by the public authority under the GDPR. The public authority must then provide an overview of the personal data of the data subject processed as well as a description of the purpose for which the data is being collected and with whom (which organisations) the data have been shared.[17] A similar practise exists under the Police Data Act and the Act on Judicial and Criminal Data. For example, art. 25 para 1 sub c of the Police Data Act states:

> *The data subject has the right to obtain from the controller, at the data subject's written request within six weeks, a determination about the processing of personal data concerning him or her and, where that is the case, to access those personal data and to obtain information on whether the police data relating to this person have been disclosed for a period of four years prior to the request and has a right to information on the recipients or categories of recipients to whom the data have been disclosed, in particular recipients in third countries or international organisations (…).*

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?

---

[16] To answer this question, we have taken a look at the rights of the data subject in the following laws: Legal and Criminal Records Act (*Wet justitiële en strafvorderlijke gegevens*), the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten*), the Police Data Act (*Wet op de politiegegevens*) and the Passport Law (*Paspoortwet*).

[17] Article 15 GDPR.

One of the requirements as set out in the parliamentary letter of 2003 is clarity with regard to the liability for erroneous data in the Basic Registrations.[18] As explained above, the holder of a registration is responsible for the accuracy of the information in a Basic Registration. If a public authority is in doubt as to the correctness of certain data, the user has a duty to report to the holder of the Basis registration (see also the answer to question 1).[19] A public authority that has no reason to doubt the accuracy of the data and uses the data from the basic registration, acts in accordance with relevant requirements.

The liability of the malfunctioning of national information networks is governed by art. 6:162 Civil Code. Theoretically, both the controller, the partner institution who uses the data in the information system and the institution who is responsible for supplying the wrong data, might be liable for any false information entered into the system. The government has given an example where the liability of the partner institution might be at stake: an authority who uses data which are labelled 'under investigation', might be liable when it uses these data without any further research.[20]

In some cases, there are specific legal provisions on liability. For example, the Land Registry (*Kadaster*) is considered to be the main source for obtaining information on the (legal) status of registered property. The Land Registry is engaged in (inter alia) the maintenance of the public registers, the keeping and updating of the register records, topography, large-scale topography and the management of the rural facilities. The Land Registry also has the task of providing information on the data obtained by the Land Registry in the exercise of its task. In respect of faults committed by the Land Registry in connection with the keeping and updating of the various registrations and the provision of information, the latter is subject to a special liability regime laid down in Article 117 of the Land Registry Law. Under article 117 of the Land Registry Act, inter alia, the Land Registry is liable towards data subjects for all errors, omissions, delays or other irregularities (of its officials) in, inter alia:

- drawing up or issuing copies, extracts and certificates from the public registers,
- the provision of information (in paper form and electronic form) from the basic register of land registration and registrations for ships and aircraft;
- provision of information (in paper form and electronic form) as to geographical information.

However, article 117 of the Land Registry Act explicitly provides that, in the performance of his public tasks, the Land Registry is not liable for damage resulting from the provision of data derived from third parties and found to be materially inaccurate, or the lack of timely receipt or disclosure of data *originating from third parties by acts or omissions by third parties*. This exclusion from liability has been motivated by the fact that the data concerned

[18] See requirement No. 1.4 from the letter of parliament, 2002/03, 26 387, No. 18, p. 12.
[19] Letter of parliament 2002/03, 26 387, No 18, p. 13.
[20] *Kamerstukken II* 2005/06, 30656, 3, p. 17.

come mainly from individual municipalities. The Land Registry is therefore not liable for any damage caused if and by reason of the fact that a municipality did not fulfil its obligations under the law with regard to the transmission of data to the Land Registry or did not do so to a sufficient degree. The Government took the view that this would not necessarily mean that the municipality in question would be liable. That would depend on whether the inaccuracies in the data were required to the customers to give rise to reasonable doubts as to the accuracy of those data. It follows that, in the absence of a specific civil liability regime, the action of the municipality in question will be assessed in the light of the provisions of Article 6:162 of the Civil Code, in particular the unwritten law.[21]

There is not much case law on this subject, although one Court of Appeal-case might be mentioned. This case concerned the Land Registry Act which we just mentioned. In this case, the Court of Appeal judged that both a notary (a user of the Land Registry) and the holder (the Land Registry Authority (*Kadaster*)) were liable in the case where a notary used data which were not accurate: it used the wrong information that a right of mortgage was established for an amount of € 3 million, instead of € 4 million. This was a mistake of the Land Registry, which had thus committed a fault in the sense of art. 6:162 Civil Code. The Court further ruled that the notary who used these data had also acted wrongful. The notary should not only have used the information in the Land Registry, but should have also studied the deed which established the right of mortgage. The Court did not express itself on the amount to which both the Land Registry and the notary were liable.[22]

Background: In the legal framework of some European information systems the legislator established a substitutional liability or subrogation mechanism (Art. 48 SIS II-Regulation (EC) 1987/2006; see also Art. 116(2) Convention Implementing the Schengen Agreement; Art. 40(2), (3) CIS-Regulation 515/97). Art. VI-40 ReNEUAL Model Rules formulates a general rule along these lines in order to enhance the protection of individuals facing damages caused by such mechanisms. In addition, Art. VI-40(2) provides for a compensation mechanism among the participating authorities in order to provide incentives to comply with their respective legal obligations.

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

---

[21] See S.A.L. van der Sande, *Overheidsaansprakelijkheid voor het verstrekken van onjuiste informatie* (diss. RU), Kluwer 2019, p. 170-173.
[22] Court of Appeal Amsterdam, 20-10-2015, ECLI:NL:GHAMS:4327.

There is no discussion in the Dutch legal doctrine on specific legal safeguards with information sharing as mentioned in the question. Apart from the obligation to report back any wrong information (*terugmeldvoorziening*) there are no other specific safeguards or legal remedies. However, the lack hereof has been the subject of report of the Court of Audit (*Algemene Rekenkamer*) in 2014 and 2019.[23] This Court has taken a look at the ten Basic Registrations. One of its findings is that the principle of "single gathering and multiple use" is efficient and effective from the point of view of public authorities. This principle can also benefit citizens and businesses, who do not have to provide the same data for each and every personal situation. However, the reverse is that people can lose sight and grip on their own data. In the view of the Court of Auditors, within the basic registration system too little is done to put citizens and businesses at the heart of the system. The Court notes a lack of a concerted and unambiguous provision that enables citizens and businesses to see what data is available to the public, which provision should also offer insight into what data the government uses and shares and which should allow incorrect data to be corrected. In the current situation, a citizen might become aware of the inaccuracy of his or her data in the registration and he might, for this reason, be denied a certain provision. In that case, the citizen will have to go to the holder of the basic registration himself in order to enter or correct his data. The Court of Auditors has also made a plea in favour of a single contact point for problems and errors, which can also effectively resolve problems and errors. This is especially necessary in a society which is largely digitally driven, according to the Court, since this makes it 'easy' for mistakes to be repeated.

In his reaction, the Minister of the Interior and Kingdom Relations stated that he has no plans to make a single contact point with authority and mandate to correct errors. The actual recovery of errors would thus remain the responsibility of the organisations that manage (basic) registrations and of the organisations that take decisions with legal effects for citizens. However, a motion by Parliament was adopted which noted that where citizens are affected by errors in the basic registrations without any wrongdoing on their part, it is desirable to establish an authoritative central reporting point where citizens are able to report and resolve problems with the basic registrations. This provision should also be able to actively accompany and support the rectification of incorrect data. The motion was unanimously accepted by Parliament and will thus lead to a single provision where citizens can report problems with basic registrations and correct errors.[24]

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

[23] Algemene Rekenkamer, *Grip op gegevens: het stelsel van basisregistraties voor burgers en bedrijven*, June 2019 (*Grip on data: the Basic Registrations System for citizens and businesses*) and *Rapport basisregistraties*, October 2014.

[24] Parliamentary Documents II 2018/19, 26 643, No. 630. (*Motion van der Molen/Middendorp*) and the response of the minister in a letter to parliament concerning a Central reporting point for incorrect registrations in Basic Registrations', 25th of November 2019, Ref. 2019-0000616399.

authorities? Are you aware of ongoing court proceedings concerning such matters? What are most important cases or principles established in this case law?

There is case-law of the Council of State in which the principle of sincere cooperation with the European Union (Article 4 (3) TEU) is the basis for data exchange between foreign administrations in the EU. Three examples are given below.

In the judgment of 6 August 2003[25] the dispute concerned the decisions of the Dutch Media Authority in which both the Luxembourg and the Netherlands authorities claim to exercise supervision over the programmes of RTL 4 and RTL 5, while it is established that the Directive 97/36/EC excludes double supervision.
The Council considers that the decision taken by the Authority cannot be maintained, since it is contrary to the purpose, scheme and scope of the Directive and, in the light of that, and in view of the fact that Luxembourg has been monitoring appellant's control over many years under the Directive 97/36/EC. In doing so, the Authority did not sufficiently demonstrate the principle of sincere cooperation with the Community (Article 10 of the EC Treaty). In its judgment the Council referred to the judgments of the Court of Justice of the EU in Cases C-115/00 (Hoves) and C-178/97 (Banks).[26]

In the judgment of 18 January 2012[27], the third country national was not in the possession of the correct residence permit as a result of the refusal by Spain. She claimed in Spain that she had asked to issue a long term residence permit complying with the requirements laid down in Article 8 (3) of the Long-Term Residents' Directive 2003/109/EC, but only obtained a certificate. She also claimed that Spain failed to implement the Directive in time and that there was the judgment of the Court of Justice of 15 November 2007 in which Spain was convicted as it had failed to implement this Directive.[28] In those circumstances, the Dutch authorities ought to have carried out an inquiry into the documents submitted to it, or to enquire with the Spanish authorities about her status, according to the foreign national. The Council of State understands the foreign national's claim to require the Dutch authorities to waive the obligation to submit a long term residence permit pursuant to the 'hardship clause'.

Under the principle of sincere cooperation with the European Union (Article 4 (3) TEU) the Dutch authorities may be required to carry out further examination in the context of the application of the hardship clause, for example where a foreign national has proved plausibly not to be in possession of the EU long term residence permit, because a Member State has failed to implement the directive correctly or has failed to implement it correctly or does not apply it correctly. However, according to the Council of State a mere assertion by a foreign

[25] Council of State 6 August 2003, ECLI:NL:RVS:2003:AI0788 (RTL case): the principle of sincere cooperation is applied between foreign governing bodies in media cases.
[26] The Council of State took into account recitals 68 to 71 in the Hoves judgment and recitals 37 and 40 to 42 and 45 in the Banks judgment.
[27] Council of State 18 January 2012, ECLI:NL:RVS:2012:BV1586 (EL Haddad): the principle of sincere cooperation between foreign administrative authorities regarding the long-term residents permit.
[28] CJEU 15 November 2007, Case C-59/07, Commission v Spain.

national that she is in distress, on the ground that a Member State refuses to issue an EC residence permit, is not sufficient for that purpose.

In the judgment of 21 February 2019[29] the illegal third country national had an entry ban imposed by Belgium for the duration of ten years. Afterwards The Netherlands re-issued an entry ban for the duration of five years. In this dispute the central question was whether the Dutch authorities had the power to impose an entry ban as the illegal third country national already had an entry ban which was issued by the Belgian authorities. As an entry ban deprives the illegal third country national of access to stay and re-enter in the territory of all the Member States his stay in the Netherlands was unlawful.[30] The Council of State considered that it was contrary to the principle of legal certainty that the Dutch authorities issued an entry ban against the illegal third country national, whereas the Belgian authorities had already issued an entry ban. According to the Council of State in the light of the principle of sincere cooperation (Article 4 (3) TEU) the Dutch authorities should, after becoming aware of the entry ban issued by the Belgian authorities, have consulted with those authorities and, if necessary, refrain from issuing the entry ban.

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?

There are three judgments of the Council of State in which the judgment of the Court of Justice in Case C-503/03 Commission v Kingdom of Spain [2006] is applied.

In two judgments of 7 October 2008[31] and 12 September 2008[32], the Council concluded that Article 27 (2) of Directive 2004/38/EC should be interpreted in accordance with the consistent case law of the Court on the interpretation of the concept of public order as set out in Article 3 of Directive 64/221/EEC. According to the judgment of the CJEU of 31 January 2006 Case C-503/03 Commission v Kingdom of Spain [2006] , that interpretation applies also to cases where the foreign national is a national of a third country who is married to a national of a Member State.

In the judgment of the Council of State of 26 January 2010[33] there is a explicit reference to paragraph 36 of the judgment of 31 January 2006 in Case C-503/03 Commission v Kingdom of Spain [2006] , in order to clarify that Article 5 (2) of the Schengen Convention is the same as Article 5 (4) (c) of the Schengen Borders Code (allowing third-country nationals to enter its territory).

---

[29] Council of State 21 February 2019, ECLI:NL:RVS:2019:565: the principle of sincere cooperation between foreign administrations when imposing an entry ban on illegally staying third-country nationals.
[30] CJEU 26 July 2017, Case C-225/16, Ouhrami, ECLI:EU:C:2017:590, paragraph 50.
[31] Council of State 7 October 2008, ECLI:NL:RVS:2008:BG1209.
[32] Council of State 12 September 2008, ECLI:NL:RVS:2008:BF1415.
[33] Council of State 26 January 2010, ECLI:NL:RVS:2010:BL1460.

There is no national case law on article 25 (2) of the SIS II Regulation .

Background: see Question I.5.

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?

No.

Background: see Question I.7.

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).

There is no discussion in the Dutch legal doctrine on specific legal safeguards with cross-border or multi-level information sharing. However, we can draw the attention on a research in 2017 of the Dutch Data Protection Authority carried out into the SIRENE Bureau of the Police. This agency is responsible for the exchange of information with the EU Member States on alerts in SIS II.

In February 2017, the Data Protection Authority published the results of their research into the SIRENE Bureau of the Police.[34] As far as the SIS II alerts are concerned, the SIRENE Bureau is not coordinating alerts pursuant to Article 24 of the SIS II Regulation on quality control. The SIRENE Bureau acts in breach of Article 7 (2) of the SIS II Regulation. This also leads to the conclusion that the SIRENE Bureau acts in breach of Article 4 (1) of the Police Data Act , because the person in charge has not taken sufficient measures to ensure that the police data are accurate in view of the purposes for which they are processed.

The Data Protection Authority finds that the deletion of additional data from SIRENE files complies with Article 12 (4) of the SIS II Regulation and the SIS II Decision, pursuant to

34 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_rapport_db_sirene_10_januari_2017.pdf

which the records which include the history of alerts shall be deleted one to three years after the deletion of the alerts. Article 38 of the SIS II Regulation and Article 53 of the SIS II Decision are also complied with where the second paragraph stipulates that personal data stored by the SIRENE Bureau following an exchange of information in files shall be stored no longer than the period necessary to achieve the purpose for which they were supplied. They shall in any event be deleted at the latest one year after the related alert has been deleted from SIS II. Article 1.16 of the SIRENE Manual, which provides, inter alia, that personal data stored by the SIRENE Bureau following the exchange of information in files pursuant to Article 12(4) of the SIS II legal instruments is, in any event, to be deleted at the latest one year after the deletion of the SIS II alert.

The Data Protection Authority found that the police are not sufficiently aware of the SIS alerts. Among other things, it was found that the police did not fulfil their work processes and procedures.

The Data Protection Authority found that the police are not sufficiently aware of the SIS alerts. Among other things, it was found that the police did not fulfil their work processes and procedures.

Following this research by the Data Protection Authority, the police took several measures to process the police data in SIS II correctly and accurately. These include better monitoring of alerts. Furthermore, people from different police units working with the system are familiar with their knowledge, developments and best practices. Finally, the police carried out a quality check in 2018, taking into account the findings of the Data Protection Authority. As a result of these improvements, the Data Protection Authority did not see any reason to intervene again.

Furthermore it is interesting to mention the reference which is made by the district court of Haarlem on 5 March 2019 in Case K.A. to the Court of Justice .[35]

In both cases, the claimants have applied for a family visit visa in the Netherlands. The Minister for Foreign Affairs has refused to grant this visa, against which decision the claimant has lodged an objection and appeal. The visa has been refused because the claimants are considered by one or more Member States as a threat to public order as defined in the Schengen Borders Code or in the international relations of one or more Member States. Claimants have respectively the Syrian and Egyptian nationality, but both visa applications have been processed by the Dutch representations in Jordan. After consultation within the meaning of the Visa Code, Germany and Hungary respectively objected to the issuing of the visa. In Case C-226/19, Germany claims that Germany objected to the fact that, in the past, it obtained a short stay visa in Germany by way of a payment to an intermediary. However, this visa has not been registered by the German Embassy. In Case C-225/19, an application lodged by the applicant for a short stay in Hungary has been rejected in the past. It is not

[35] District Court Harlem 4 March 2019, ECLI:NL:RBDHA:2019:2097.

clear to him why. No alert in the Visa Information System for the purposes of refusing entry to the Schengen area has been entered for both claimants in the Schengen Information System for the purposes of refusing entry into the Schengen area.

In these cases the visa is not refused on the basis of the Visa Information System (VIS) or the Schengen Information System (SIS).Claimants are also excluded from such systems. The referring court is therefore uncertain as to how the ground for rejecting the refusal can be assessed in the appeal against the refusal and whether such a review constitutes an effective remedy. In national case-law, in similar situations it has been assumed that there was an adequate remedy in the other Member State against the objection of that other Member State. However, there was a European alert. In other judgments, it has been held that such proceedings do not exist or are insufficient. In the final negative decisions the respondent has not indicated whether and how claimants can challenge the objection in Germany and Hungary respectively. The content of the objections of those Member States is also not established. Furthermore, it is not clear whether the German/Hungarian authorities took a decision against claimants concerning public order. Since the referring court cannot itself examine that ground for refusal itself, it therefore asks whether, in that situation, there is no breach of, in particular, Articles 41 and 47 of the Charter of Fundamental Rights of the EU (EU Charter). In addition, he doubts whether the reference to a procedure in another country is compatible with the one-stop-shop principle.

The preliminary ruling questions are formulated as followed:

In the case of an appeal as referred to in Article 32(3) of the Visa Code 1 against a final decision refusing a visa on the ground referred to in Article 32(1)(a)(vi) of the Visa Code, can it be said that there is an effective remedy within the meaning of Article 47 of the EU Charter under the following circumstances:

- where, in its reasons for the decision, the Member State merely stated: ‘you are regarded by one or more Member States as a threat to public policy, internal security, public health as defined in Article 2.19 or 2.21 of the Schengen Borders Code, or to the international relations of one or more Member States’;
- where, in the decision or in the appeal, the Member State does not state which specific ground or grounds of those four grounds set out in Article 32(1)(a)(vi) of the Visa Code is being invoked;
- where, in the appeal, the Member State does not provide any further substantive information or substantiation of the ground or grounds on which the objection of the other Member State (or Member States) is based?

In the circumstances outlined in Question 1, can there be said to be good administration within the meaning of Article 41 of the EU Charter, in particular, because of the duty of the services concerned to give reasons for their decisions?

a. Should Questions 1 and 2 be answered differently if, in the final decision on the visa, the Member State refers to an actual and sufficiently clearly specified possibility of appeal in the other Member State against the specifically named authority responsible in that other Member State (or Member States) that has (or have) raised the objection referred to in Article 32(1)(a)(vi) of the Visa Code, in which that ground for refusal can be examined?

b. Does an affirmative answer to Question 1 in connection with Question 3(a) require that the decision in the appeal in and against the Member State that made the final decision be suspended until the applicant has had the opportunity to make use of the option of appealing in the other Member State (or Member States) and, if the applicant does make use of that option, until the (final) decision on that appeal has been obtained?

   For the purpose of answering the questions, does it matter whether (the authority in) the Member State (or Member States) that has (or have) objected to the issuing of the visa can be given the opportunity, in the appeal against the final decision on the visa, to act as second defendant and on that basis to be given the opportunity to introduce a substantiation of the ground or grounds on which its objection is based?