Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: United Kingdom

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

UK Supreme Court Response to Questionnaire

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

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.

Yes. The Digital Economy Act 2017 (the "DEA 2017") sets out in Part 5 additional statutory powers in a framework which enable data to be shared for particular public interest purposes, subject to consistent safeguards and new offences that help protect personal information, as well as the GDPR and data protection legislation. Prior to the DEA 2017, the legal framework in respect of data sharing was found across a complex range of common law and statutory provisions, conferring powers to share information often in very specific circumstances and subject to a range of different conditions and restrictions. The DEA 2017 contains particular provisions designed to combat fuel poverty and provided for new powers to disclose information to gas and electricity suppliers related to fuel poverty.

In 2018, under the DEA 2017, the Department for Digital, Culture, Media & Sport, the Cabinet Office, the Home Office, and the UK Statistics Authority produced the Information Sharing Code of Practice: Public Service Delivery, Debt and Fraud (the "Part 5 Code"), which provides a set of principles and guidance for the use and disclosure of information under these powers.

The Part 5 Code refers to the pre-existing data-sharing code produced by the Information Commissioner's Office ("the ICO", the UK data regulator) and envisages data sharing agreements taking multiple forms, including a reciprocal exchange of data (likely to fall within Book VI-2(1)) and the pooling of information by several organisations to make it available to them all (which is likely to fall within Book VI-2(3)).

Examples of existing mechanisms of information exchange include the following:

The National Referral Mechanism (NRM) is an online system aimed at identifying and referring potential victims of modern slavery and ensuring they receive the appropriate support. This is likely to fall within Book VI-2(1).

The Education and Skills Funding Agency (ESFA) Information Exchange, which is a secure, online system that provides a platform for academies, ages 16-to-19 education providers, high needs providers and local authorities to do business with ESFA. This is also likely to fall within Book VI-2(1).

The Extremism Analysis Unit (EAU) of the Home Office is a cross-government resource that government departments can use to commission research and analysis of extremism in this country and abroad where it has a direct impact on the UK and/or UK interests. The EAU

draws on information from both public and private sources and therefore receives data shared by other government departments. This does not appear to fit within either of the three categories envisaged in Book VI-2 since it is more of an *ad hoc* analytical resource than an information exchange mechanism.

The UK Government also provides public access to a large amount of data as part of its commitment to open government (see data.gov.uk). This is likely to come within the type of mechanism contemplated by Book VI-2(3), although access to it is not restricted to national authorities and it can be used by members of the public.

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.

There are 29 pilot data sharing agreements between local councils and HMRC to manage and reduce council tax debt. The pilot data shares aim to help to manage and reduce council tax arrears. develop local councils' recovery procedures, identify customers whose circumstances make them vulnerable and provide them with appropriate advice and support, and enforce appropriate recovery action. The pilots involve the sharing by the local authorities of names, addresses and contact or forwarding addresses of council taxpayers who have received a liability order for failure to pay council tax disclosed and by HMRC certain tax return data.

There are also information sharing agreements between Companies House and HMRC exploring differences in filed company accounts; involving Homes England to explore potential fraud in the Help-to-Buy Scheme; a pilot agreement between HMRC and local authorities to counter fraud under the National Fraud Initiative; and a pilot scheme testing the feasibility of data matching between the Valuation Office Agency and Department of Work and Pensions data for improved fuel poverty targeting.

A register of these sharing agreements is published by the UK Government online (at https://www.registers.service.gov.uk/registers/information-sharing-agreement-0001).

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?

Yes. In the context of data sharing among public authorities, the Part 5 Code provides that a public authority must conduct a privacy impact assessment if it wishes to share data under the public service delivery, debt and fraud powers. A privacy impact assessment is a process which helps identify and reduce the privacy risks of an information sharing agreement. The ICO's *Conducting Privacy Impact Assessments Code of Practice* provides guidance on a range of issues in respect of these assessments, including the benefits of conducting privacy impact assessments and practical guidance on the process required to carry one out. The privacy impact assessment should be reviewed at critical milestones and updated where necessary (for example when a pilot under the debt or fraud power has demonstrated benefit and is to be upscaled).

The Part 5 Code is to be read alongside the *Data Sharing Code of Practice* produced by the ICO (the "ICO Code") pursuant to section 121 of the DEA 2017. The ICO Code recommends that an organisation, when considering sharing data, should consider its overall compliance

with data protection legislation and, as a first step, should decide whether to carry out a Data Protection Impact Assessment ("DPIA") (i.e. a privacy impact assessment). Under the Data Protection Act 2018, where a type of processing is likely to result in a high risk to the rights and freedoms of individuals, the controller is obliged, prior to the processing, to carry out a DPIA, which is an assessment of the impact of the envisaged processing operations on the protection of personal data (s.64). Even if not legally obliged to carry one out, the ICO recommends that organisations consider following the DPIA process.

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?

In *R (Butt) v Secretary of State for the Home Department* [2019] EWCA Civ 256, [2019] 1 W.L.R. 3873, the claimant sought judicial review of the collection, recording and sharing of information relating to him by the EAU, contending it unjustifiably interfered with his right to privacy under Article 8 of the European Convention on Human Rights. The Court of Appeal held that the EAU's collection and storage of publicly available information about an individual would only engage that individual's Article 8 right if: (1) that individual had a reasonable expectation of privacy in respect of the information; and (2) the collection and storage of the information was systematic. In the present case, neither condition was satisfied, since the information was publicly available and EAU's collection had not been systematic.

The Supreme Court considered the sharing of personal data between public bodies in the Scottish case of *Christian Institute v Lord Advocate* [2016] UKSC 51. The appeal was primarily concerned with a devolution issue, specifically whether provisions of a Scottish act, the Children and Young People (Scotland) Act 2014 (the "Act") were within the legislative competence of the devolved Scottish Parliament. A related issue was a provision in that Act that encouraged information sharing between public bodies in order to achieve its public-service objective. The Court considered that such sharing may well constitute an interference with the Article 8 ECHR right to family and private life, raising the question of whether the measure could be justified under Article 8(2). In order to be "in accordance with the law" the measure must have a basis in domestic law and precise enough to give legal protection against arbitrariness. Here, the powers and duties of disclosure set out in the Act had to be read alongside the Data Protection Act 1998 ("DPA 1998"), which significantly curtailed the information-sharing provisions. The Court took the view that there were very serious difficulties in accessing the relevant legal rules, given that one had to read together and cross refer between the Act and the DPA 1998. Further, there were a lack of safeguards, since the Act and its guidance did not require the provision of any notification to the data subject of the information sharing. As a result the Court concluded that the information-sharing provisions did not meet the Article 8 criterion of being "in accordance with the law". In addition, the Court held that the information-sharing measure was disproportionate. Though the DPA 1998 contained safeguards on the sharing of sensitive personal data (when correctly read with the Act), the Act did not maintain a fair balance in relation to the disclosure of confidential non-sensitive personal data, given the lack of any consent or notification requirements.

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?

The DEA 2017 does not contain provisions dealing with these specific issues. As a matter of general law, a decision-making body has to make a rational assessment of the weight and reliability of information available to it from any source.

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 the answer to 5.a) above.

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

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

No, but information about all information sharing agreements concerning England-only or non-devolved bodies for a disclosure or group of disclosures under the public service delivery, debt and fraud powers must be submitted to the Government Digital Service (GDS) in the Cabinet Office, which maintains a searchable register available to the general public. This register contains details of the information sharing agreement, including a short description of the purpose of the information sharing agreement, whether consent from the citizen is required and, if so, whether consent has been obtained, the specific objective where the public service delivery provisions are used, description of the information being disclosed and by which body, including bodies outside the public sector, the method by which data will be disclosed, the bodies receiving the data, including bodies outside the public sector, how long the information will be held, when the data sharing agreement will come into effect and when it will end.

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 DEA 2017 does not contain specific provisions to this effect. Under general data protection laws an individual could make a subject access request regarding their personal data to the providing and receiving bodies.

See the decision of the Supreme Court in *Christian Institute* discussed above.

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?

The DEA 2017 does not contain provisions dealing with these specific issues. General domestic law includes rights in relation to protection of reputation (the law of defamation) and data protection law includes rights to compensation in relation to misuse or misrecording of personal data.

8. In your national legal order, are there any specific safeguards or legal remedies of individuals considering information about them to be false or an exchange of

information about them to be illegal? Is there a political or academic discussion about (further) needs for new or more specific legal safeguards in this context? Are there any recent legislative proposals on this topic?

The DEA 2017 creates a criminal offence where the recipient of personal information received under the Part 5 powers discloses that information knowingly or recklessly, unless the disclosure falls within a specific set of circumstances (including being required by statute, court order, or EU obligations, for the purposes of a criminal investigation, for journalism in the public interest, or disclosed with the consent of the person to whom it relates) (s. 41).

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?

We are not aware of detailed judgments on EU mechanisms of advanced cross-border or multi-level information exchange among European authorities. However, EU mechanisms such as the Schengen Information System have been mentioned in extradition cases including *Sobczyk v Poland* [2017] EWHC 3353 (Admin), *Gulan v Regional Court in Gliwice (Poland)* [2018] EWHC 3369 (Admin), and *Zimackis v General Prosecutor's Office (Latvia)* [2017] EWHC 315 (Admin).

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?

Commission v Spain has been mentioned in a number of cases but not considered in detail (see for instance *Fatima v Secretary of State for the Home Department* [2019] EWCA Civ 124, [2019] 1 W.L.R. 3207; *National Crime Agency v N* [2017] EWCA Civ 253, [2017] 1 W.L.R. 3938).

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?

We are not aware of judgments dealing with these particular provisions.

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?

We are not aware of any specific proposals for new safeguards. There are a number of legal safeguards in the existing legislation, including in the Data Protection Act 2018 (the "DPA

2018”). These safeguards were recently considered in the case of *R (El Gizouli) v Secretary of State for the Home Department* [2019] EWHC 60 (Admin), in which the High Court considered whether the provision of mutual legal assistance to a foreign state in support of a criminal investigation that could lead to prosecution for offences that carry the death penalty violated the DPA 2018. The Court in essence held that the data was collected by the police in the UK for a criminal investigation and it was at least likely that the purpose of the investigation always envisaged a foreign prosecution of some sort given that the alleged crimes were committed abroad. There was nothing incompatible with the purpose for which data might be processed in a UK police investigation with using it for a foreign prosecution. The applicable data-transfer provisions in the DPA 2018 had been followed, with the non-fatal exception of a failure to inform the ICO, and in any event the case fell within the exception in the DPA 2018 allowing for transfer abroad in individual cases for specific law enforcement purposes. The case is under appeal to the Supreme Court.