Bundesverwaltungsgericht

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

Leipzig, Germany

Answers to questionnaire: Ireland

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

Response of the Supreme Court of Ireland

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.

Response:

It is noted that Book VI (Administrative Information Management) of the ReNEUAL Model Rules on EU Administrative Procedure applies to the following categories of information management activities of public authorities based on EU law:

(a) exchange of information according to a structured information mechanism (viz. "a pre-defined workflow allowing authorities to communicate and interact with each other in a structured manner beyond the general obligations of mutual assistance according to Book V" per Art VI-2(1)),

(b) exchange of information under a duty to inform without prior request,

(c) establishment and use of a database.

The Data Sharing and Governance Act 2019

The Data Sharing and Governance Act 2019 ("the 2019 Act") was signed into law on the 4th March 2019 but as of the date of this response a limited number of its provisions (as mentioned below) have come into operation. The 2019 Act, *inter alia*, seeks to provide a legal basis on which public bodies may engage in sharing of personal data for defined purposes (see reference to section 13(1)) below), subject to certain safeguards and administrative and technical requirements. Pending full implementation of the 2019 Act, public bodies may, generally, only disclose information in a specific circumstance or for a specific purpose permitted or required under Irish or EU law.

Outline of the Act

The following are the substantive Parts of the 2019 Act.

- **Part 2 of the 2019 Act (containing sections 5 to 12) specifies the scope of the Act's application: notably it does not affect the operation of data protection law and does not apply to data sharing for various purposes as set out in section 12[1].**

---

[1] Viz. (a) the prevention, detection or investigation of offences,
(b) the apprehension or prosecution of offenders,
(c) the imposition or execution of a fine or sentence of imprisonment,
(d) the exercise of the functions of the Criminal Assets Bureau,
(e) protecting the security of the State including, but not limited to, the following:
(i) preventing, detecting and investigating offences under the Offences against the State Acts 1939 to 1998, the Criminal Law Act 1976, the Criminal Justice (Terrorist Offences) Act 2005 and the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010;
(ii) protecting the State from—
(I) espionage,
(II) sabotage,
(III) unlawful acts that subvert or undermine, or are intended to subvert or undermine, parliamentary democracy or the institutions of the State, and
(IV) acts of foreign interference that are, or are intended to be, detrimental to the interests of the State and are clandestine or deceptive or involve a threat to any person, whether directed from, or committed or intended to be committed within, the State or not,
(f) identifying foreign capabilities, intentions or activities within or relating to the State that impact on the international or economic well-being of the State,

- **Separately, individual provisions of the 2019 Act make clear that they are not intended to displace specific statutory regimes affecting data sharing by public bodies or any provision of EU law.**

- **Part 3 of the 2019 Act (containing sections 13 and 14) regulates data-sharing.**

- **Part 4 (containing sections 15 to 22) provides for the concluding of data-sharing agreements between public bodies.**

- **Part 5 (containing sections, *inter alia*, gives Government Ministers power to collect and process specified information regarding public servants arising from their membership of a public service pension scheme.**

- **Part 6 (containing sections 33 to 36) regulates the disclosure of business information by a public body to another public body.**

- **Part 7 (containing sections 37 to 42) regulates databases, copyright in which is owned by a public body, designated as base registries to act as authoritative sources in respect of information frequently used by public bodies in the performance of their functions and imposes obligations on the public body designated as the base registry owner e.g. to ensure insofar as is reasonable that the information held on the base registry is accurate, up to date and complete and to put in place appropriate administrative and technical measures to control and monitor access to the base registry (see section 38(1)).**

- **Part 8 (containing sections 43 and 44) authorises the establishment of an information system for the purpose of enabling a data subject to exercise his or her rights under GDPR and view information in relation to any personal data breaches relating to him or her.**

- **Part 9 (containing sections 45 to 68) provides, inter alia, for the establishment of a Data Governance Board to oversee various aspects of the operation of the 2019 Act.**

Application of the Act to categories specified in the ReNEUAL Model Rules

---

(g) co-operating with authorities in other states and international organisations aimed at preserving international peace, public order and security,
(h) the defence of the State, or
(i) the international relations of the State.
Subject to Part 5, the 2019 Act does not apply to the disclosure by a public body to anotherpublic body of the personal data of a data subject for the internal administrative purposes (including relating to the employment of the data subject concerned)of the first or second mentioned public body.

The 2019 Act would appear, insofar as its provisions regulating data sharing are concerned, to apply to all three of the categories of information management activities of public authorities listed at (a) to (c) above, as section 9 of the 2019 Act provides:

> **"9. (1) In this Act, "data-sharing" means the disclosure of information, including personal data, by a public body to another public body.**
>
> **(2) For the purposes of this Act, an addition or change to the information held on an information system under the control of a public body that results automatically from an addition or change to information held on an information system under the control of another public body, is deemed to be a disclosure by the second mentioned public body to the first mentioned public body of the information so added or changed on the information system under the control of the first mentioned public body." (emphasis added)**

Notably, section 13(2) in Part 3 of the 2019 Act envisages that a public body ("the first mentioned public body") may disclose personal data to another public body ("the second mentioned public body") only where—

> **(a) the personal data concerned is disclosed—**
>
> > **(i) for the purpose of the performance of a function of the first or second mentioned public body, and**
> >
> > **(ii) for one or more of the following purposes:**
> >
> > > **(I) to verify the identity of a person, where the first or second mentioned public body is providing or proposes to provide a service to that person;**
> > >
> > > **(II) to identify and correct erroneous information held by the first or Second mentioned public body;**
> > >
> > > **(III) to avoid the financial or administrative burden that would otherwise be imposed on a person to whom a service is being or is to be delivered by the first or second mentioned public body were the second mentioned public body to collect the personal data directly from that person;**
> > >
> > > **(IV) to establish the entitlement of a person to the provision of a service being delivered by the first or second mentioned public body, on the basis of information previously provided by that person to the first mentioned public body (or another public body that previously disclosed the information to the first mentioned public body);**
> > >
> > > **(V) to facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;**
> > >
> > > **(VI) to facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;**
> > >
> > > **(VII) to enable the evaluation, oversight or review of a service,**

programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;

(VIII) to facilitate an analysis of the structure, functions, resources and service delivery methods of the first or second mentioned public body,

(b) the personal data concerned is disclosed under and in accordance with a data sharing agreement entered into between public bodies as authorised by Part 4 of the 2015 Act.

(c) the first and second mentioned public body—

(i) comply with the rules, procedures and standards, if any, prescribed under section 64 of the 2019 Act,

(ii) have regard to any guidelines issued by Minister for Public Expenditure and Reform under section 65 of the 2019 Act, and

(iii) where a model data-sharing agreement has been prepared or revised under section 66(3) of the 2019 Act, comply with that subsection,

(d) in a case in which the second mentioned public body is engaged for gain (i.e. profit) in the production, supply or distribution of goods or the provision of services, the use by that public body of the personal data could not lead to the distortion of competition in trade in those goods or services within Ireland,

(e) the personal data concerned has been lawfully obtained and held by the first mentioned public body, and

(f) the personal data concerned is disclosed in accordance with (i) any other provisions of the 2019 Act applicable and (ii) any other enactment or law of the European Union applicable to the first or second mentioned public body, and

(g) the disclosure of the personal data is—

(i) necessary for the performance of the functions in relation to which the information is being disclosed, and

(ii) proportionate in the context of the performance of those functions and the effects of the disclosure on the rights of the data subjects concerned.

Oversight of these arrangements will be provided by a newly established Data Governance Board ("Board").

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.

Response:

An example of an additional mechanism of information exchange in Ireland is a special statutory regime governing the sharing of information relating to the Personal Public Service Number ("PPS Number"). The PPS Number is designed for use in transactions between the individual and public bodies and is intended to be used for the purpose of accurately identifying the individual in the administration of public services. The PPS

Number may only be used by persons authorised to do so by statute law (as mentioned below) and data may only be shared using the PPS Number as a common identifier where the sharing is authorised by statute law e.g. Data Protection or Social Welfare law.

The Social Welfare (Consolidation) Act 2005 (as amended) ("the 2005 Act") regulates the allocation and use of the PPS Number. Only public bodies specified in the 2005 Act may use the PPS Number. An informally consolidated version of the 2005 Act as amended is available at: https://www.welfare.ie/en/downloads/RunningConsolidation-of2005Act.pdf

Under section 262(6) of the 2005 Act:

(a) Where a "specified body" (i.e. a public body specified in the list of public bodies contained in Schedule 5 of the 20005 Act) has a transaction with a person, the Minister for Social Protection may share the Information in the PPS Number of a person (the person's "public service identity") with the specified body <u>to the extent necessary in respect of that transaction for authentication by the specified body of the person's public service identity</u>.

(b) A specified body may use a person's public service identity in performing its public functions <u>insofar as those functions relate to the person concerned</u>.

Sections 265 to 270 of the 2005 Act regulate the circumstances in which and conditions under which specified bodies may share information for various purposes.

At a more general level, section 265(2) of the 2005 Act authorises a specified body holding information to share that information with another specified body who has a transaction with a natural person relating to a relevant purpose, where the specified body seeking the information provides the personal public service number of the person who is the subject of the transaction and satisfies the data controller controller of the specified body holding the information that the information requested is relevant to the transaction for that purpose between the person and the specified body seeking the information. Section 265(3) of the 2005 Act provides that a specified body may only seek information for the purposes of a transaction relating to a relevant purpose.

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?

Response:

1. Public bodies which are data controllers are subject to the GDPR obligation, given fuller effect by section 84 of the relevant domsetic legislation, the Data Protection Act 2018[2], to conduct a data protection impact assessment (DPIA) where having regard to

[2] Available at: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

its nature, scope, context and purposes, a type of processing and in particular a type of processing using new technology, is likely to result in a high risk to the rights and freedoms of individuals. Where no data protection impact assessment has been carried out in relation to processing proposed to be undertaken under a proposed data sharing agreement between public bodies, each of the proposed parties to a proposed agreement will require to publish on a website accessible to the public a summary of the reasons why no data protection impact assessment has been carried out (section 55(1)(c) of the 2019 Act).

2. The Irish Data Protection Commission ("DPC") has issued a guide for public bodies in relation to data sharing in the public sector, available at: https://www.dataprotection.ie/sites/default/files/uploads/2019-05/190418%20Guidance%20on%20Data%20Sharing%20in%20the%20Public%20Sector.pdf

In summary, that guidance recommends that all data sharing arrangements in the public sector should generally:

- **have a basis in primary legislation;**
- **have a clear justification for each data sharing activity;**
- **make clear to individuals that their data may be shared and for what purpose;**
- **be proportionate in terms of their application and the objective(s) to be achieved;**
- **share the minimum amount of data to achieve the stated public service objective;**
- **have strict access and security controls; and**
- **ensure secure disposal of shared data.**

More specifically with reference to Question 3, the DPC guidance recommends that from the outset when assessing a data sharing arrangement (either as a provider, a recipient, or both) public bodies should undertake the following <u>non-exhaustive</u> checks:

- **identify what the arrangement is meant to achieve. (The guidance states that all data sharing arrangements should have a clearly understood set of objectives which are documented and recorded).**
- **identify whether the objective could be achieved without sharing the data or by anonymising it. (The guidance states that the default position should be to analyse whether personal data needs to be shared in the first instance in order to achieve the goal(s)).**
- **identify the minimum information required to achieve that purpose. (The guidance states that all data sharing arrangements should share only the minimum required personal information to achieve the body's objectives).**
- **identify any risks which the data sharing may pose. (The guidance states that when considering whether to implement and place a data sharing agreement on a legislative footing consideration should be given of the fact that such sharing could increase the reluctance of individuals to provide accurate personal data to**

public sector bodies. It should also take account of any disproportionate negative impact on particular sections of society).

- **identify when and how often the data should be shared. (The guidance states that it is good practice to document this and set out whether the sharing arrangement will be ongoing or periodic or whether it will occur in response to a particular set of events).**
- **consider whether a Data Protection Impact Assessment (DPIA) is required. (The guidance states that DPIAs can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect a public body or the individuals it engages with).**

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?

Response:

As far as can be ascertained, there are no decisions of the Supreme Court of the other Superior Courts of Ireland (the High Court and Court of Appeal) specific to the operation of advanced information exchange between public bodies.

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?

Response:

This question is so widely framed as to render it difficulty to answer accurately. It is not clear whether "decision-making body" is intended to refer exclusively to a court or extends to other non-judicial bodies. Insofar as court proceedings are concerned, ordinarily, information in a <u>domestic</u> public register will only be admissible in evidence in a court as *prima facie* proof of its content (a) if the statutory regime concerned provides that it be so admissible and (b) then only to the extent that evidence to the contrary has not been admitted which disproves that content.

There are examples of the application of this approach to <u>legal documents or acts</u> of foreign authorities, e.g. in the context of the criminal justice mutual assistance regime: where property has been confiscated in a designated foreign State in any proceedings on foot of an Irish court's confiscation order, a certificate purporting to be issued by a competent authority in the designated State under a request made to that State and stating (a) that property has been realised pursuant to the request, (b) the date of realisation, and (c) the proceeds of realisation, is admissible, without further proof, as evidence of those matters (see section 49(4), Criminal Justice (Mutual Assistance) Act

2008). However, it should not be concluded from this that an Irish court would not in other circumstances/under another legal framework require to have the veracity of information emanating from a foreign public authority subjected to proof according to the ordinary law of evidence.

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.

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?

Response:
See 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?

Response:

In answering this question, we take the question to ask whether our national legal order provides for "..the automatic…informing of the person concerned?". Persons whose data is processed within the meaning of the GDPR or Law Enforcement Directive (the latter as transposed into Irish law by Parts 5 and 6 of the Data Protection Act 2018) would have such rights to be informed as derive from those instruments.

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?

Response:
Persons whose data is processed within the meaning of the GDPR or Law Enforcement Directive (the latter as transposed into Irish law by Parts 5 and 6 of the Data Protection Act 2018) would have such rights of access to their personal data as derive from those instruments.

Section 44

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.

Response:

This question is too widely drafted to allow for a correct answer to be provided: the correct answer would entirely depend on various factors, including the particular information exchange regime concerned and the source of the malfunctioning or false information.

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?

Again, this question is too widely drafted to allow for a correct answer to be provided: the correct answer would entirely depend on the particular information exchange regime concerned. Data subjects have the right to rectification, erasure of personal data and restriction of processing under the GDPR and the Law Enforcement Directive (the relevant provisions of the latter having been transposed into in Irish law by section 92 of the Data Protection Act 2018) and associated remedies, including the remedy of a data protection action founded on tort (under sections 117 and 128 of the Data Protection Act 2018, as appropriate).

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?

Response:

We are not aware of any decision of the Irish courts touching on the operation of such mechanisms.

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.
Response:
We are not aware of any decision of the Irish courts drawing on these legal sources. Currently, Ireland is not connected to SIS II. Ireland, via An Garda Síochána (the Irish police), is currently running a project to connect Ireland to SIS II. The aim of the project is to go technically live in December 2019 and to be operationally connected with the SIS II data-base in early 2020.

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.
Response:
See preceding response.

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).

Response:
Section 44 of the Data Sharing and Governance Act 2019 – which has not yet come into legal effect - envisages that the Minister for Public Expenditure and Reform may, with the approval of the Government, establish an information system for the purpose of enabling a data subject to—

(a) exercise his or her rights under the GDPR, and

(b) view information in relation to the personal data breaches, if any—

(i) which affect his or her personal data, and

(ii) in respect of which a notification has been made for the purposes of Article 34(1) of the GDPR.

It is envisaged that the information system will incorporate a website (to be known as the "Personal Data Access Portal") which may include facilities by means of which a data subject may—

(a) view personal data relating to him or her held by a public body, together with the information relating to that personal data referred to in Article 15 of the GDPR,

(b) view information in relation to the personal data breaches, if any—

(i) which affect his or her personal data, and

(ii) in respect of which a notification has been made for the purposes of Article 34(1) of the GDPR,

(c) view a copy of a data-sharing agreement under which his or her personal data has been disclosed between public bodies, and

(d) send a request to a public body in relation to the exercise by him or her of the rights provided for in Articles 15, 16, 17, 18, 19, 20 and 21 of the GDPR.