Data Storage by Public Administrations*

Gherardo CARULLO** & Christian ERNST***

Keywords: public administration, databases, digitalization, data storage, outsourcing, internalization, digital sovereignty

1 INTRODUCTION

Public administrations often process vast amounts of data.[1] As noted by the European legislator, the public sector 'collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, political, economic, legal, geographical, environmental, meteorological, seismic, touristic, business, patent-related and educational areas'.[2]

In dealing with public administration and data, it is therefore possible to start the analysis taking for granted that the collection, possession and consumption of large data-sets, including those containing personal data, is an immanent feature of the powers entrusted to public authorities. After all, it would be difficult to imagine that, for example, the so-called civil registries[3] could not manage personal data. It would be even less realistic to maintain that such civil registries could not

---

* Parts 1-3 and 7 are by Dr Gherardo Carullo. Parts 4-6 are by Dr Christian Ernst.

** Senior lecturer and adjunct professor at the University of Milan; PhD in Administrative Law from the same University; LL.M. from King's College, London. Email: gherardo.carullo@unimi.it.

*** Professor of Public Law at the Helmut-Schmidt-University/University of Bundeswehr Hamburg; Habilitation at Bucerius Law School Hamburg; doctorate from University of Kiel. Email: christian.ernst@hsu-hh.de.

1 There is a broad consensus in the literature on this aspect, *see* amongst others: Ines Mergel, R. Karl Rethemeyer & Kimberley Isett, *Big Data in Public Affairs*, 76 Pub. Adm. Rev. 928–937 (2016). Stéphane Lavertu, *We All Need Help: 'Big Data' and the Mismeasure of Public Administration*, 76 Pub. Adm. Rev. 864–872, 864–872 (2016). Artem A. Kosorukov, *Digital Government Model: Theory and Practice of Modern Public Administration*, 20 J. Leg. Ethical Regul. Issues (2017).

2 *See* recital 8 of Directive 2019/1024/EU on open data and the reuse of public-sector information.

3 Expression with which we intend to refer to the registers held by public administrations containing some of the essential data on natural persons, such as date of birth, residence, etc. In Italy, e.g. a new fully digitalized register called '*Anagrafe Nazionale della Popolazione Residente*' ('National Register of Resident Population', ANPR) has recently been established. In Germany, the '*Melderegister*' ('Register of residents') is based on a federal law since 2015. In the time before the 'Bundesländer' (federal states) had the legislative competence. The federal legislator pursues with this standardization, among other things, an effective realization of e-government.

Carullo, Gherardo & Ernst, Christian. 'Data Storage by Public Administrations'. *European Public Law* 26, no. 3 (2020): 545–568.

exist at all. The same reasoning may apply to any other set of information needed to carry out a public power, such as tax collection.

The digitalization of public administrations results in these large data-sets being increasingly processed wholly or partly by automated means.[4] In Italy, for example, this phenomenon is well described by the most recent statistics made available by the Agency for Digital Italy (AgID). Among the 21,368 administrations considered, even taking into consideration only the 13,807 (64.6%)[5] that have fulfilled the burden of communicating the list of their databases, there are currently 159,724 databases in use in the public sector.[6] In Germany, the digitalization of the public administration has so far developed hesitantly in comparison to other European countries. More recently, the shift towards digitalization has become increasingly important, as shown not only by the numerous government initiatives and commissions, but also by the number of electronically submitted tax returns, for example. Between 2010 and 2017, the number of electronically submitted tax returns increased by 156% from 8.6 million to 22.1 million.[7]

Therefore, we can assume that, from a context in which information was stored on article, in physical archives, the public sector has shifted, or is rapidly shifting, towards a context in which such information is contained in digital databases.

2 DIGITAL DATA MANAGEMENT: ESSENTIAL CONCEPTS

2.1 Grounds for collecting personal data relevant in the public sphere

One of the fundamental provisions of Regulation 2016/679/EU (General Data Protection Regulation(GDPR) or the Regulation) is that processing of personal data is lawful only if and to the extent that at least one of the conditions provided by Article 6(1) applies.

Articles 6(1)(a) and 6(1)(b) provide respectively that processing is lawful if 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes', or if 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. Within agreements between private parties, it is indeed normally assumed that the user can refuse a given privacy policy, or to some extent deny his consent to certain uses, eventually by

4 *See* Mergel, Rethemeyer & Isett, *supra* n. 1.

5 According to the statistical data provided by the AgID at the address, www.agid.gov.it/agenda-digitale/open-data/basi-dati-pa/dati-statistici.

6 Number of databases in use in Italy in the public sector obtained from the 'Statistics/Data Analysis' system made available by AgID at the address, http://basidati.agid.gov.it.

7 Statista-Dossier, *e-Government* 11 (2018).

relying on a competing solution that provides greater guarantees regarding the processing of personal data.

There are certain circumstances, however, in which this scenario can be significantly different. Self-determination regarding the choice of granting consent to the processing of personal data can sometimes be reduced or even eliminated. In this regard, it is possible to identify at least three different orders of situations in which this happens within the public sector.

First, the acquisition of data is sometimes connatural to the administrative activity to be carried out. In this regard, the GDPR provides specifically that processing of personal data is lawful if it 'is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', as provided for by EU or national law.[8] As explained by the European legislator itself, in such cases 'a law as a basis for several processing operations … may be sufficient'[9] and 'it should also be for Union or Member State law to determine the purpose of processing'[10] as well as:

> whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.[11]

For example, tax data is usually collected either through statements sent to the competent authority from the data subject, or via different means by the administration itself.[12]

The data subject has a limited choice on whether granting or not consent to the processing of his or her personal data also in those situations in which the processing is required upon the data controller by law. In this regard, the GDPR provides that processing of personal data is lawful if it 'is necessary for compliance with a legal obligation to which the controller is subject', as provided for by EU or national law.[13]

In other cases, the situations in which consent should be acquired is of such a nature that, in reality, the data subject has no choice but to provide the

---

8 *See* Art. 6(1)(e) and Art. 6(3)(a, b) GDPR.
9 Recital 45 GDPR.
10 *Ibid.*
11 *Ibid.*
12 For example, in Italy, Attachment no. 1, Table no. 2 of the Regulation of the *Agenzia delle Entrate* adopted in implementation of Arts 20 and 21 of Legislative Decree of 30 June 2003, n. 196, on the protection of personal data provides that the Agency may acquire data from interested parties or third parties, and may also acquire it through the interconnection and the comparison of data with other administrations, such as the *Guardia di Finanza* (Financial Police).
13 *See* Art. 6(1)(e) and Art. 6(3)(a, b) GDPR.

information. This happens, for example, where vital interests are at stake. As a matter of fact, the GDPR provides that processing of personal data is lawful if it 'is necessary in order to protect the vital interests of the data subject or of another natural person'.[14] This situation might occur, for example, in relation to the provision of health services. If the data subject is unconscious, such provisions of the GDPR may apply. On the other hand, the data subject, when conscious and fully capable of taking an informed decision, still has a very limited choice, insofar as denying consent to the processing of data would (potentially) lead to fatal or irreparable consequences.

After data acquisition, come into play multiple additional activities that public administrations must perform to manage the information that they have acquired. Before going on to analyse such activities, it is worth clarifying the difference between the concept of data and information.

2.2 Meaning of data

When dealing with information stored in digital databases, a very important distinction,[15] derived from computer terminology, is the one between the concept of *data* and that of *information*.

The definition of data provided by the International Organization for Standardization (ISO) offers a useful technical approach to such distinction. In the ISO vocabulary on information technology, data is defined as a 'reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing'.[16] Data is therefore described as a separate concept from that of information. The latter is the result of the reinterpretation of what is represented by the former.

Another particularly useful technical definition of data emphasizes that, 'from a business process design perspective, data, information, and knowledge serves purposes that are quite different from each other'.[17] Data is used to store and transfer information and knowledge, so that 'data will only become information or

---

[14] *See* Art. 6(1)(d) GDPR.

[15] The expression is by Diana Urania Galetta, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, Federalismi.it 1 (2016). The Author refers to the need felt by the author to maintain this distinction in commenting the Italian Legislative Decree on administrative transparency.

[16] *See* definition n. 2121272 referred to in the vocabulary of the document of the International Organization for Standardization and the International Electrotechnical Commission ISO/IEC 2382: 2015, www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en.

[17] Ned Kock, *Systems Analysis & Design Fundamentals: A Business Process Redesign Approach* (SAGE Publications 2006). In this sense, from a broader perspective on the relationship between data and information, cf. also Trevor Haywood, *Info Rich – Info Poor: Access and Exchange in the Global Information Society* (Bowker-Saur 1995).

knowledge when they are interpreted by human beings or in some cases, artificial intelligent agents'.[18]

In legal literature, on the basis of such technical definitions, it has been explained that while data is always a known element, information has a subjective connotation. Information is what the user from time to time derives from the aggregation of data that can be obtained by consulting a database.[19]

For public administrations, this means that data is an asset through which it is possible to acquire the information needed to carry out the tasks with which they are entrusted.

The distinction between data and information is of particular importance for our purposes because we focus on the technical notion of *data*, that is, as an element susceptible to being stored, manipulated and transferred, independently of its ability to represent information.

It is worth noting though that this approach does not contend that data is devoid of any informative relevance. Rather, it means that data, from our point of view, comes into play not because of the information it is suitable to represent, but because of the (multiple) activities necessary to handle and make use of it.

For this reason, the concept of data can also be distinguished from that of an electronic document.[20] The latter concept refers to any medium – immaterial, in the case of electronic documents[21] – in which some piece of information can be stored, within the meaning that we have outlined above.[22]

Therefore, as we consider data in its technical meaning, i.e. a sequence of *bits*, such a notion can encompass also the one of electronic documents, which are to be stored on a physical device as data. It is for this reason that what mostly matters for our purposes is not the information represented by data, but rather the data itself and the operations that can be processed over such data.

---

18 *Ibid*.

19 The citation is by Galetta, *supra* n. 15. *See also* Alfonso Masucci, *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, 50 Riv. Dirit. Civ. 749 (2004). The latter Author stresses the fact that information is not data and that the data itself does not convey any meaning, being merely the starting element from which information is processed.

20 According to Art. 3(1)(35) of Regulation 2014/910/EU, '"electronic document" means any content stored in electronic form, in particular text or sound, visual or audiovisual recording'.

21 It is such, according to the definition in Art. 3(1)(35) of Regulation 2014/910/EU, '*any content stored in electronic form, in particular text or sound, visual or audiovisual recording*'.

22 Article 23-*ter* of the Italian Code of Digital Administration, related to digital administrative documents, clarifies that data and digital documents held by public administrations constitute primary and original information.

2.3 The data supply chain

Data, as defined above, can be the subject of multiple operations of different types, nature and purposes. To identify the various activities that may come into play for the management, organization, use and dissemination of data, we can consider those referred to in the definition of the term 'processing' provided by the GDPR.

According to the Regulation, 'processing':

> means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[23]

The list of activities is very broad and, according to the wording of Article 4(2) itself, is not exhaustive. Additionally, these activities are not all equally relevant and do not necessarily need to be carried out by the same subject.

By grouping the various operations listed in the above cited definition by their aim, we can outline four macro categories: (1) activities aimed at acquiring data ('collection'); (2) conservation activities, in a broad sense ('organization', 'structuring' and 'storage'); (3) activities aimed at saving, modifying, reading or deleting stored data ('recording', 'adaptation', 'alteration', 'retrieval', 'restriction', 'erasure', 'destruction'); and, finally, (4) activities aimed at the consumption of data ('consultation', 'use', 'disclosure by transmission', 'dissemination or otherwise making available', 'alignment', 'combination').

These categories are in line with 'the value chain of commercial re-use of PSI [Public Sector Information]', which 'is composed of four elements; these are 1) data creation, 2) aggregation and organization, 3) processing, editing and packaging and 4) marketing and delivery'.[24]

Based on these categories, we can therefore assume that the data supply chain is composed of – at least – four different elements: i) data acquisition/creation; ii) data storage, including aggregation and organization; iii) data manipulation, including data editing and packaging; and iv) data consumption.

---

[23] Article 4(1)(1) GDPR.

[24] *See* the document 'Digital Broadband Content: Public Sector Information and Content', dated 30 Mar. 2016 (DSTI/ICCP/IE (2005) 2/FINAL, www.oecd.org/sti/36481524.pdf) of the Directorate for Science, Technology and Industry Committee for OECD Computer and Communications Policy. In relation to the specific supply phase, the subdivision is also reflected in the European legislation, where the 'supply' of the data is mentioned. In this regard, *see* recital 2 of Regulation 2010/268/EC governing access to spatial data sets and related services within the INSPIRE system referred to in Directive 2007/2/EC, which aims to '*ensure a coherent approach to the provision of access to spatial data sets and services*'.

3 IMPLEMENTING THE PRINCIPLES OF PROTECTION BY DESIGN AND BY DEFAULT IN THE DATA STORAGE PHASE IN THE PUBLIC SECTOR

The proposed breakdown of the four phases involved in data management processes allows us to analyse separately the organization and the structuring of the different activities that come into play in each. This approach can thus be compared to the one that was made possible by the unbundling process that took place in network industries.[25] By analysing each group of activity separately, it is possible to evaluate the legal framework applicable to each element of the data supply chain, and thus assess what measures could or should be applied to each.

The various activities of each phase of the data supply chain may be organized and structured according to multiple different methods. Depending on the choices made by each administration, or by the legislator, it can be possible to have a single system in charge of carrying out all the activities, or as many systems as the aforementioned phases are, or even more.

At this regard, an important role is nowadays played by the *data protection by design and by default* principles.[26] In short, the principle of protection by design entails that the processor should implement appropriate technical and organizational measures to ensure data protection. The latter principle, on the other hand, requires that 'by default, only personal data which are necessary for each specific purpose of the processing are processed'.[27]

To comply with those principles, as clarified by the GDPR itself, the controller should adopt internal policies and implement appropriate measures, such as 'minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features'.[28]

In particular, the GDPR suggests that, to comply with the principles of privacy by design and of privacy by default:

> when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into

[25] Among the numerous sectors affected by this process, we can mention: telecommunications, cf. Directive 90/388/EEC and subsequent Directives; electricity, cf. Directive 96/92/EC and subsequent Directives; gas, *see* Directive 98/30/EC and subsequent Directives; rail transport, *see* Directive 1991/401/CE and subsequent Directives; civil aviation, *see* Directive 87/601/EEC, and subsequent provisions on the matter.

[26] *See* Art. 25 GDPR.

[27] *See* Art. 25(2) GDPR.

[28] *See* Recital 78 GDPR.

> account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations'.[29]

Finally, the same recital also provides that 'the principles of data protection by design and by default should also be taken into consideration in the context of public tenders'.[30]

To meet such requirements, it should therefore be duly assessed if, and to what extent, it would be appropriate to outsource, fully or partially, some of the activities of the data supply chain. It would also need to be assessed to what extent it can be deemed possible to entrust to third parties the realization of certain infrastructures, or the provision of certain assets needed to carry out the activities involved in the data supply chain, or to entrust to third parties the provision of the services aimed at making such data consumable.

A similar approach has also been suggested by the Research Network on EU Administrative Law (ReNEUAL) in their ReNEUAL Code.[31] The Authors have proposed a specific regulation on access to information, which they have considered 'an important aspect of the concept of "privacy by design"'.[32] As part of the Model Rules of the ReNEUAL Code, it has been proposed that for each information obligation or database, clear and complete rules must be laid down regarding the authorities that can access such information and use it and to the conditions under which it is allowed to access and use it.[33]

In order to implement a data protection system from the design stage, each phase of the *data supply chain* must be considered individually so that it is possible to evaluate the risks, and thus the most appropriate mitigating measures to be taken for it. In other words, it is necessary to evaluate specific solutions for each activity that, depending on the type of data involved, can guarantee that personal data is processed in a way that ensures both the protection required by the GDPR and the fulfilment of the specific administrative function to be exercised.

In light of the above-mentioned data supply chain, we can now assess where such data can be stored.

---

[29] *See* Recital 78 GDPR.

[30] *See* Recital 78 GDPR.

[31] The ReNEUAL Code, as explained by the Authors, represents a project with the aim of identifying the most suitable paths to translate the constitutional values of the European Union into rules on the administrative procedure concerning the non-legislative implementation of Union law and of European policies, Paul Craig et al., *Libro I – Disposizioni generali*, in *Codice ReNEUAL del procedimento amministrativo dell'Unione Europea* 1 (Giacinto Della Cananea et al. eds, Editoriale Scientifica 2016).

[32] Diana Urania Galetta et al., *Libro VI – Gestione delle informazioni amministrative*, in *Codice ReNEUAL del procedimento amministrativo dell'Unione Europea* 197 (Giacinto Della Cananea et al. eds, Editoriale Scientifica 2016).

[33] *Ibid*.

4 OUTSOURCING DATA STORAGE TO THE PRIVATE SECTOR

In the field of data storage, many private Information and Communications Technology (ICT, or IT) companies offer their services to the public sector. Since in this case the administration does not have to build up its own technical skills, resources and infrastructure, accepting a private offer could mean saving costs.[34] However, scepticism remains. The German Federal Police, for example, stores the images of its newly acquired body cams on an Amazon Cloud.[35] Amazon is not only the leading player in online retailing, but is also a leading international provider of cloud computing operating under the name of Amazon Web Services (AWS).

This raises the question as to whether it is compatible with constitutional principles that a private company stores recordings which were made by police officers during their operations. Should the administration make use of public IT service providers instead, whose number on the market is increasing constantly?

As no explicit European legal regulation exists regarding this question, the legal situation in the individual Member States varies widely. In Austria, for example, where the digitalization process of public administration is rather advanced, the '*Bundesrechenzentrum GmbH*' (Federal Computing Centre) is entrusted by law with various public tasks. Besides performing tasks imposed by the Federal Act on the Bundesrechenzentrum GmbH,[36] the Bundesrechenzentrum GmbH plays an essential part in the process of implementing electronic legal transactions and operating the electronic land register. Bundesrechenzentrum GmbH is 100% state-owned.

In Germany, on the other hand, a central public IT service provider does not even exist at the federal level. Rather, some individual governmental divisions at the federal, state and municipal level have established independent public companies to perform the given tasks. One may find sporadic and heterogeneous regulations of particular cases in which the public administration is allowed to make use of private IT service providers. Tax administration, for example, may only seek help from computer centres which are part of a fiscal administration authority.[37] In contrast, data used for the electronic land register can be processed not only by the competent court, but also by another government agency, and even by a legal entity under public law.[38] Moreover, of all sensitive data, a private IT company may provide its services within the framework of electronic criminal

---

[34] Torsten Gründer, *Partnerschaftsgestaltung für sicheres IT-Outsourcing*, 40 Datenschutz Datensicherheit – DuD 667–674, 667 (2016).
[35] German Parliament Document No. 19/8180, at 28.
[36] § 2 para. 3 Austrian Federal Act on the Bundesrechenzentrum GmbH, BGBl. No. 757/1996.
[37] § 17 para. 3 and § 2 para. 2 Financial Administration Act, BGBl. I 2006, s. 846.
[38] § 126 para. 3 of the Land Register Regulations, BGBl. I 1994, 1114.

records. It can thus be entrusted with storing electronic files in a legally binding manner, provided that a public body actually and solely controls the physical and electronic access to the company's data processing equipment.[39] Interpreting this literally, members of a public authority would have to actually control access to the data processing equipment itself – i.e. the concrete computers and not only the private company headquarters. While it is doubtful that these requirements are even feasible,[40] it is yet another question if the provision is legally permissible.

Are state authorities therefore permitted to release data from their sole sphere of influence, which is characterized by public law? Are they simultaneously allowed to give a private individual at least indirect access to the data, for example through the actual power of disposal over a physical data medium?[41] From the point of view of data protection law, the access would regularly be a processing on behalf of a controller ('Processor' – Article 28 GDPR), although this aspect will be left aside for the question of legal admissibility.

5 PRINCIPLE OF DIGITAL SOVEREIGNTY

The prohibition of entrusting public administrations' data to private IT service providers can be based on three elements: the character of obligatory state tasks, the state's enabling responsibility ('*Gewährleistungsverantwortung*') and finally the confidence in the integrity and functionality of state structures and institutions. The principle of digital sovereignty results from their overall view.

5.1 Obligatory state tasks

Although obligatory state tasks are typically not listed explicitly, it is widely recognized that there exist some inalienable state tasks that are based on elementary state functions.[42] Traditionally, these include legislation and justice, internal and external security, law enforcement and financial management.[43] Data processing

[39] § 497 para. 1 Code of Criminal Procedures.

[40] Critical also Ritscher, *§ 497,* in *StPO – Kommentar zur Strafprozessordnung* 1 (III ed., Helmut Satzger, Wilhelm Schluckebier & Gunter Widmaier eds, Eschborn 2018).

[41] About the sphere of influence *see* Marcus Griesser & Werner Buntschu, *Vertrauen oder Wissen? Eine Risikobetrachtung für sicheres IT-Outsourcing*, 40 Datenschutz Datensicherheit – DuD 640–646, 645 (2016).

[42] Compare Josef Isensee, *Staatsaufgaben*, in *Handbuch des Staatsrechts*, vol. IV, 117–160, marginal no. 27-marginal 31 (3d ed., Josef Isensee & Paul Kirchhof eds, C.F. Müller 2006). Alexander Thiele, *Art. 33 Abs. 4 GG als Privatisierungsschranke. Zugleich Anmerkung zum Urteil des Niedersächsischen Staatsgerichtshofs vom 05.12. 2008, 2/07*, 49 Staat 274–298, 279 (2010).

[43] Compare Josef Isensee, *Staatsaufgaben*, in *Handbuch des Staatsrechts* vol. IV, 117–160, marginal no. 28 (Josef Isensee & Paul Kirchhof eds., 3 ed., C.F. Müller 2006). Hans Peter Bull, *Die Staatsaufgaben nach dem Grundgesetz* 102 (1973). Hans Peters, *Öffentliche und staatliche Aufgaben* 892 (C.H. Beck 1965). Helmuth Schulze-Fielitz, *Grundmodi der Aufgabenwahrnehmung*, in *Grundlagen des Verwaltungsrechts*, vol.

itself could be an obligatory state task as well – for instance, in the context of the register of residents. Although the data collected and used there usually fulfil a merely supportive function for other governmental tasks,[44] data processing itself is the primary state task of operating the State's register of residents.[45] The category of an obligatory state task is indicated by the considerable and substantially importance for the fulfilment of the tasks of the state's administrative and the fact that the data may be highly sensitive. If operating the register of residents is seen as an obligatory state task, it must not be permissible to outsource the concerned data to private individuals.

Involving private IT service providers in the storage of administrative data may also be inadmissible if the data and their use are not an obligatory state task themselves, but an integral part of other obligatory state tasks. In order to be an integral part of an obligatory state task, the data must be essential to its performance. This means that the performance must 'stand and fall' with the data, for instance due to their necessary availability and processing.[46] The more central data are for the performance of an obligatory state task, the less privatization can be considered.

As digital information technologies are becoming ubiquitous, data are now of particular importance in almost all areas of administration. A criterion for assuming that data are an integral part of a specific state task may be the question of whether data have not just acquired their significance through the availability of digital information technologies but have always been an elementary and traditional part of the performance of tasks. Accordingly, case files kept by civil courts could fulfil these requirements. Jurisprudence is an obligatory state task, without the data processing itself being the primary task to be fulfilled. For centuries, however, data processing in the form of file management has played a major role in judicial activity. Hence, data processing can be classified as an integral part of the obligatory state task of jurisprudence and can therefore not be left to private individuals.

I marginal no. 95 (2nd ed., Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, & Andreas Voßkuhle eds, C.H. Beck 2012). Gunnar Folke Schuppert, *Staatswissenschaft* 292 (Nomos 2003).

44 Dirk Heckmann & Frank Braun, *Datenverarbeitung durch private IT-Dienstleister im Meldewesen*, Bayer. Verwaltungsblätter 581–586, 584ff. (2009). Compare Isabell Conrad & Marc Strittmatter, *§ 22*, in *Handbuch IT- und Datenschutzrecht*, marginal no. 203 (2nd ed., Astrid Auer-Reinsdorff & Isabell Conrad eds, C.H. Beck 2016).

45 Heckmann & Braun, *supra* n. 44, at 584.

46 Compare Thomas Petri & Dorfner Claudia, *E-Justiz und Datenschutz – Ausgewählte Rechtsfragen*, 3 Z. für Datenschutz 122–128, 127 (2011).

5.2 State enabling responsibility

Outsourcing public administrations' data to private IT service providers may also be inadmissible if the authorities are not able to sufficiently control and monitor the provider. This concept of an enabling responsibility of the state ('*Gewährleistungsverantwortung*') demands that the state must ensure that tasks are performed in accordance with the public interest and common good, even if private parties are involved in the performance of state tasks. The state's responsibility can even make the state retrieve the task and carry it out itself again if the private provider's work was not satisfactory.[47] Thus, an object-related approach to tasks is replaced by a more flexible concept of responsibility, which can capture the interaction between the state and the private sector more appropriately.[48] The concept of enabling responsibility regularly requires a legislative balancing decision, which always includes the estimation of how effective control and monitoring of private actors can actually be ensured.[49] If the private sector fails, it must be possible for the state to effectively take over the tasks itself again.

In order to fulfil its enabling responsibility in the area of IT outsourcing, the state must consider the specific risks of data handling. In accordance with the traditional purposes of legal protection, as they exist in data protection law pursuant to Article 4 no. 12, Article 32(2) GDPR and the former Article 17(1) Directive 95/46/EC, and regarding the specific risks we can differentiate between the availability, falsification, inappropriate use and publication of data. The state must therefore ensure that the data which it requires in order to perform its tasks are always available.[50] A loss of data or even a temporary unavailability regularly leads to an extensive loss of administration capabilities in practice. For the public administration's day-to-day work, it is equally important that the integrity of the

---

47 Compare for the various levels of responsibility e.g. Wolfgang Hoffmann-Riem, *Verantwortungsteilung als Schlüsselbegriff moderner Staatlichkeit,* in *Staaten und Steuern, Festschrift für Klaus Vogel zum 70. Geburtstag* 47–64, 47 et seq. (Paul Kirchhof et al. eds, 2000). Gunnar Folke Schuppert, *Der Gewährleistungsstaat – modisches Label oder Leitbild sich wandelnder Staatlichkeit?*, in *Der Gewährleistungsstaat: ein Leitbild auf dem Prüfstand* 11–52, 25 et seq. (Gunnar Folke Schuppert ed., Nomos 2005). Helmuth Schulze-Fielitz, *§ 12*, in *Grundlagen des Verwaltungsrechts*, marginal no. 150 et seq. (Wolfgang Hoffmann-Riem, Susanne Baer & Andreas Vosskuhle eds, C.H. Beck 2006).

48 Andreas Voßkuhle, *Gesetzgeberische Regelungsstrategien der Verantwortungsteilung zwischen öffentlichem und privatem*, in *Beyond Privatization and 'Slender' State* 47–90, 57 (Gunnar F. Schuppert ed., Nomos 1999). Claudio Franzius, *Der 'Gewährleistungsstaat' – ein neues Leitbild für den sich wandelnden Staat?*, 42 Der Staat 493–517, 493 (504ff.) (2003).; Schuppert, *supra* n. 43, at 292.

49 Hans-Christian Röhl, *Verwaltungsverantwortung als dogmatischer Begriff?*, in *Verwalt. Beih.* 33–56, 54 (1999).

50 Compare Walter Ernestus, *§ 9*, in *Bundesdatenschutzgesetz*, marginal no. 156 et seq. (8 ed., Spiros Simitis ed., Nomos 2014). Philipp Kramer & Martin Meints, *Art. 32*, in *DSGVO BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze*, marginal no. 25 (Herbert Auernhammer, Philipp Kramer & Kai von Lewinski eds, Carl Heymanns Verlag 2017). Silke Jandt, *Art. 32*, in *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG*, marginal no. 27 (Jürgen Kühling & Benedikt Buchner eds, C.H. Beck 2017).

data's content as a requirement for its decisions' substantive legality be preserved. However, due to the data complexity, an individual administrator can hardly conclusively verify the accuracy of data in content so that the risk of falsification is high. Furthermore, the state's actions are restricted significantly by the principle of using data only for specific und explicit purposes, which is stated, for example, in Article 5(1)(b) GDPR. Passing on the data to additional actors can increase the risk of inappropriate use, especially if these actors pursue their own objectives. For instance, private IT service providers could use the data to evaluate the usage behaviour of their customers, to improve their own systems or to research new systems. It has become a basic principle of data economics that available data will be used. Finally, it is necessary to prevent the unauthorized disclosure of government data, in particular those relating to core areas of government activity or personal information.

The necessary level of enabling responsibility is not only determined by data-specific risks, but also by essential features and characteristics of data. To begin with, data can be used non-rivalling, which means that, if one person uses data, it does not prevent others from using the same.[51] When data is disseminated or disclosed, it is virtually impossible, because of the possibility of digital copying, to take it back.[52] Even if one might still be able to influence the actual consequences of inappropriate usage retrospectively, this does not apply to the (inappropriate) use of data itself. If data get lost or the content is corrupted, only an additional full data record can typically help correct the data retrospectively. This has considerable consequences for the possibility of retrieving the performance of tasks by the state. In principle, the state is able to regain control over public tasks entrusted to private parties, e.g. the operation of a motorway, in order to correct errors and restore proper conditions. When dealing with data, however, due to their structural features, the negative consequences can extend irreversibly into the future.

The third aspect which the state has to consider when determining its necessary level of enabling responsibility is the general business risk. Since we cannot assume an increased risk of unlawful conduct will follow any appointment of a private individual, (normative) structural differences are becoming a decisive factor for each consideration. According to the European Court of Justice, private individuals processing personal data must provide sufficient legal safeguards to ensure effective protection against misuse as well as unauthorized access to and

---

[51] Jean Nicolas Druey, *Information als Gegenstand des Rechts: Entwurf einer Grundlegung* 33 (Schulthess 1995). Viktor Mayer-Schönberger, *Informationsrecht fur die Informationsgesellschaft*, 97 SJZ 383, 384 (2001). Helmut F. Spinner, *Ist Wissen analogiefähig?*, in *Festschrift für Jean Nicolas Druey zum 65. Geburtstag* 958 (Rainer J. Schweizer et al. eds, Schulthess 2002).

[52] Compare Mayer-Schönberger, *supra* n. 51, at 860. Jan Ole Püschel, *Informationen des Staates als Wirtschaftsgut* 41 (Duncker und Humblot 2006).

use of data.[53] Private individuals' actions regularly lack specific, legally specified official duties.[54] Furthermore, employees of private IT service providers are typically not subject to the same penalties as public officials.[55]

There are further differences between private and public IT service providers, which affect the level of enabling responsibility, that needs to be fulfilled: First, public IT service providers are supported and financed by the state, regularly without the purpose of making profit.[56] Hence, public authorities have many possibilities to supervise and influence them. Private IT service providers, in contrast, do not only lack such supervisory and influencing possibilities on the operative business, but their operational activities are also exposed to an insolvency risk.[57]

The relationship between private IT service providers and public authorities is often characterized by considerable information asymmetries to the detriment of public authorities.[58] While public administration's IT skills and knowledge necessary to effectively negotiate contracts are often underdeveloped, private IT service providers have increasingly gained considerable market power, which is further strengthened by network effects and lock-in effects.[59]

This leads to the conclusion that two different enabling responsibilities must be distinguished, one internal and one external, and that they must be determined separately in each case. The internal enabling responsibility ensures the functionality of state functions. The state must ensure that the data on which it relies in order to carry out its (administrative) tasks are available at all times and that their content is accurate. It is possible that this objective can only be achieved if the administrative data remains within the exclusive area of competence and responsibility of the state. If such data were entrusted to private individuals, they could

---

53 Case C-362/14 *Schrems v. Data Protection Commissioner (Schrems)* ECLI:EU:C:2015:650 [2015] marginal no. 91.

54 Compare BVerfG, Decision of 02 Mar. 2010, Case 1 BvR 256/08, in BVerfGE, Vol. 125, marginal no. 222, 260–385 (2010).

55 In German law, this is particularly evident in § 203 of the Criminal Code, which makes the violation of private secrets a punishable offence. Employees of private IT service providers are regularly out of the question as perpetrators.

56 In German law, this is achieved, e.g. by the legal form of an 'institution under public law'. For its liabilities, its responsible bodies are fully liable. In addition, they must guarantee the institution's operability, which, in case of doubt, is ensured by financial support, cf. Iris Kemmler, *Die Anstaltslast* 101 et seq. (Duncker & Humblot 2001). Martin Müller, *§ 86*, in *Verwaltungsrecht Band II*, marginal no. 19 (7th ed., Hans J. Wolff et al. eds, C.H. Beck 2010).

57 Griesser & Buntschu, *supra* n. 41, at 644.

58 Gründer, *supra* n. 34, at 667. Compare also Gabriel Schulz, *Informationssicherheit in Kommunen*, 39 Datenschutz Datensicherheit – DuD 466–471, 469 (2015).

59 Compare Antje Zimmerlich, *Marktmacht in dynamischen Märkten: die Abgrenzung des sachlich relevanten Marktes in Märkten der Internetökonomie* 88 (Lang 2007). Antje Zimmerlich, *Der Fall Microsoft, Herausforderungen für das Wettbewerbsrecht durch die Internetökonomie*, in *WRP* 1260–1272, 1262 et seq. (2004). Griesser & Buntschu, *supra* n. 41, at 644.

have impact on the functionality of state administration. Legal agreements can offer only limited protection against the de facto access possibilities associated with the data. There would be a risk that companies would pursue operational or political goals, especially when exposed to significant foreign influence.[60]

In addition, there is an external enabling responsibility concerning the relationship between the state and its citizens. This variant of enabling responsibility urges the state to protect the fundamental rights of its citizens focusing on personal data. Article 32 GDPR defines the level of data security necessary for data processing carried out by a processor on behalf of a controller. According to this rule, implementation costs are a criterion among others. Therefore, it is possible that in case of a private service provider one could take the pursuit of profit and successful economic action into consideration.[61] However, taking financial capabilities of private IT service providers into accout, would lead to uncertainties about the necessary level of data protection and could reward poor management. The necessary level of data protection under Art. 32 GDPR must therefore be determined objectively.[62]

In this regard, the importance of the data must be considered, e.g. their sensitivity for the individual (cf. Art. 9, 10 GDPR). On the one hand, private IT service providers may offer a higher level of protection because they have developed a considerable technical lead. On the other hand there is the risk of immense damage, especially with sensitive data. While state-owned IT service providers are bound directly to fundamental rights and public laws, the involvement of private companies can create uncertainty about responsibilities and weaken the control by public authorities, thereby already creating a significant risk for fundamental rights (cf. Art. 7, 8 CFR) that needs to be justified.[63] In principle, cost savings achieved by contracting private IT service providers are unlikely to be sufficient for this. It is therefore also possible that personal data may

---

60 Compare the manual on the so-called No-Spy decree of the BMI of 19 Aug. 2014, O4 - 11032/23#14, at 1.

61 OLG Hamburg (Higher Regional Court Hamburg), Decision of 07 July 2005, Case 1 Bf 172/03, NJW Volume 59, 310–313, 313 (2006). Jörg Hladjk, *Art. 32*, in *Datenschutz-Grundverordnung: DS-GVO*, marginal no. 5 (Eugen Ehmann & Martin Selmayr eds, C.H. Beck 2018). Carlo Piltz, *Art. 32*, in *Datenschutz-Grundverordnung: DS-GVO* 20 (Peter Gola ed., C.H. Beck 2018). Mario Martini, *Art. 32*, in *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG*, marginal no. 60 (Boris P. Paal & Daniel A. Pauly eds, C.H. Beck 2018).

62 Mario Martini, *Art. 25*, *in Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG*, marginal no. 42 (Boris P. Paal & Daniel A. Pauly eds, C.H. Beck 2018). Philipp Kramer & Martin Meints, *Art. 32*, *in DSGVO BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze*, marginal no. 35 (Herbert Auernhammer, Philipp Kramer, & Kai von Lewinski eds, Carl Heymanns Verlag 2018).

63 cf. BVerfG, Decision of 04.04.2006, Case 1 BvR 1054/01, in BVerfGE, Volume 115, pp. 320-385, 341 et seq. (2006). BVerfG, Decision of 11.03.2008, Case 1 BvR 2074/05, 1254/07, in BVerfGE, Volume 120, pp. 378-433, 397 (2008).

not leave the state's exclusive area of sovereignty and responsibility because it is the only way to ensure adequate and effective protection of fundamental rights. In this regard, the principle of digital sovereignty may complement the concepts of data protection by design and by default with a data protection by institutional structure.

5.3 Trust

Finally, there is a third way to establish the principle of digital sovereignty. Even if an explicit legal regulation typically does not exist, it is an absolutely necessary prerequisite for statehood that its citizens have trust in its work, more precisely, in the integrity and functioning of state structures.[64] Trust is widely used to refer to meeting expectations, fulfilling agreements, general confidence or reliability.[65] It becomes relevant when there is a lack of control and uncertainty.[66]

The importance of trust in the state relies on the work of John Locke. In his opinion, entering into the social contract is inseparably linked to the people's trust that the sovereign fulfils the expectations that were placed in him.[67]

---

[64] Paul Kirchhof, *Recht lässt hoffen* 91 et seq. (Beck 2014). Katarina Weilert, *Das paradoxe Vertrauen gegenüber dem Staat und seinen Institutionen*, HFR, 207 et seq. (2010). Hartmut Maurer, *§ 79*, in *Handbuch des Staatsrechts der Bundesrepublik Deutschland Band III: Demokratie - Bundesorgane*, marginal no. 11 (Josef Isensee & Paul Kirchhof eds, C.H. Beck 2005). Kyrill-Alexander Schwarz, *Vertrauensschutz als Verfassungsprinzip: eine Analyse des nationalen Rechts, des Gemeinschaftsrechts und der Beziehungen zwischen beiden Rechtskreisen* 43 (Nomos 2002). Gary S. Schaal, *Vertrauen, Verfassung und Demokratie: Über den Einfluss konstitutioneller Prozesse und Prozeduren auf die Genese von Vertrauensbeziehungen in modernen Demokratien* 11, 189 (Springer-Verlag 2013). Compare Fritz Ossenbühl, *Vertrauensschutz im sozialen Rechtsstaat*, DÖV 25–36, 25 (1972).

[65] Niklas Luhmann, *Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität* 1ff. (Lucius & Lucius 2000). Weilert, *supra* n. 62, at 208. Dirk Fox, *Vertrauen*, 39 Datenschutz Datensicherheit – DuD 328–328, 328 (2015). Ariane Berger, *Digitales Vertrauen – Eine verfassungs- und verwaltungsrechtliche Perspektive*, 132 Dtsch. Verwaltungsblatt 804–808, 805 (2017). Volker Boehme-Neßler, *Vertrauen im Internet – Die Rolle des Rechts*, 12 Multimed. Recht 439, 439 (2009). Susanne Baer, *Vertrauen: Faire Urteile in Wissenschaft und Recht* 8ff. (Wallstein Verlag GmbH 2013). Compare Rüdiger Grimm, Michaela Maier & Tobias Rothmund, *Vertrauen*, 39 Datenschutz Datensicherheit 283–288, 283 (2015). Annette Baier, *Vertrauen und seine Grenzen*, in *Vertrauen. Die Grundlage des sozialen Zusammenhalts*, 37 (Martin Hartmann & Claus Offe eds, Broschiert 2001). Margot E. Oswald, *Vertrauen – eine Analyse aus psychologischer Sicht, in Recht und Verhalten: Verhaltensgrundlagen des Rechts, zum Beispiel Vertrauen* 111 (Hagen Hof et al. eds, Nomos 1994).

[66] Compare Luhmann, *supra* n. 63, at 27 et seq. According to *Luhmann*, a relationship of trust can be important in factual terms for the reduction of complexity, in social terms for stable social interactions and in temporal terms for the continuation of such relationships. Compare Schaal, *supra* n. 62, at 64. Boehme-Neßler, *supra* n. 63, at 439. Johannes Eichenhofer, *Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz*, 55 Staat 41–67, 51 (2016). Fox, *supra* n. 63, at 328. Griesser & Buntschu, *supra* n. 41, at 641.

[67] John Locke, *Zwei Abhandlungen über die Regierung* § 149 (Suhrkamp 1977). Compare Schaal, *supra* n. 62, at 67 et seq.. Hans Huber, *Vertrauen und Vertrauensschutz im Rechtsstaat*, in *Menschenrechte, Föderalismus, Demokratie : Festschrift zum 70. Geburtstag von Werner Kägi* 193 et seq. (Ulrich Häfelin, Walter Haller, & Dietrich Schindler eds, Schulthess Polygraphischer Verlag 1979).

Nowadays, the need for trust in the proper use of digital information technologies by the state is based on two opposing forces: on the one hand, the use of relatively new technologies demands an increased degree of trust while, on the other hand, the effectiveness of traditional control mechanisms decreases.

An increased degree of trust is especially necessary if its object cannot yet point to a far-reaching history, but has only recently been developed, and so far, there is no routine or experience in dealing with it. The state administration has always worked with the traditional written form and physical files. It is only in the last three decades that digital information technologies have gained considerable influence.

In the past, the confidence placed in public authority was linked primarily to the person of the official. However, as the use of and dependence on digital information technologies increase, this personal component is becoming less important. Only a sufficient measure of trust guarantees the citizens' acceptance. If, however, the individual is not sure which data the state has access to and what happens to this data, barriers for state action arise. This applies in particular to data which the citizen cannot avoid being collected by the state. The individual loses control and her or his personal scope for action is reduced.

Parallel to this loss of trust, traditional control structures are becoming less effective. State action has traditionally and typically had a direct effect on the actual or legal situation and was therefore immediately noticeable. Collecting, using and processing data, however, is regularly excluded from direct human visibility and perception. The same applies for data being passed on and used by unauthorized third parties. In addition, it is not easy to determine whether data is incorrect, because those affected often only experience the result of data processing and cannot reconstruct the concrete decision-making process. Unauthorized publications are noticeable, but cannot be undone.[68] The use of digital information technologies is fundamentally intransparent and leads to less effective control mechanisms. However, the less control possibilities are effective, the more trust becomes important.

It is therefore a task of law to create and maintain trust through rules.[69] Since legal control of data usage in retrospect is only possible to a limited extent, trust-building legal structures must be located upstream. It is possible that legal regulations would have to make clear that certain data must not leave a public domain. In that case, a confidential handling of data requires that it is clear that the data will remain at all times within an area of responsibility characterized by an adherence to

---

[68] Compare *supra* [xxx].
[69] Boehme-Neßler, *supra* n. 63, at 439.

fundamental rights and legal obligations set forth by public law. The threshold between public and private law cannot then be crossed by IT outsourcing

6 COMPATIBILITY WITH UNION LAW

The principle of digital sovereignty understood in this way is a national constitutional requirement. As such, it must be compatible with the requirements of Union law.

6.1 Fundamental freedoms

A nationally founded principle of digital sovereignty precludes private IT service providers from being involved in the performance of state tasks. The preclusion therefore might potentially affect fundamental freedoms, namely the freedom of establishment (Article 49 of the Treaty on the Functioning of the European Union, TFEU) and the free movement of goods and services between Member States (Article 34 f. and Article 56 TFEU respectively).

In 1989, the European Court of Justice (ECJ) declared an Italian regulation incompatible with the freedom of establishment, the freedom to provide services and with the Public Procurement Directive at that time.[70] The Italian regulation stated that 'contracts with the Italian State for the installation of data processing systems on behalf of public administrations could be concluded only with companies which were directly or indirectly wholly or mainly state-owned'.[71] The ECJ, however, found that the requirement of a majority shareholding by the state could not be justified by security and control aspects.[72]

It is doubtful whether the Court's verdict would have been the same in the light of the risks of a digital information society as they have come up in recent years. Nevertheless, the fact that the decision rules that the legal requirement of a majority shareholding by the state must not be ignored. Such constellations could actually intervene at least indirectly with fundamental freedoms because shareholdings in state-owned enterprises are in fact held primarily by nationals.[73] Therefore citizens of other Member States may be impaired. In contrast to the ruling of the ECJ regarding the Italian rule that requires a majority shareholding by the state in case of involvement of private companies, the principle of digital sovereignty as proposed here effectuates a complete ban on privatization. And in

---

[70] Case C-3/88 *Commission of the European Communities v. Italian Republic (Commission v Italy)* ECLI:EU:C:1989:606 [1989] ECR 4035.
[71] *Ibid.*
[72] *Ibid.*, marginal no. 10 et seq..
[73] *Ibid.*, marginal no. 9.

that respect, there is no obligation to privatize state tasks and to not perform them exclusively with administrative resources ('make or buy'). This decision affects not even Union procurement law,[74] as not only the ECJ has meanwhile clarified in its case law on in-house procurement,[75] but as it is now also stated in Article 17 Directive 2014/23/EU and Article 12 Directive 2014/24/EU. Powers of the Member States to perform tasks themselves also derive from Article 345 TFEU, according to which European treaties do not affect the systems of property ownership of the Member States. This applies in particular to the economic policy decision on the division of tasks between the public and private sectors.[76]

In the *Essent* case, the ECJ had to rule on a Dutch regulation prohibiting any private participation in energy distribution system operators. The Court of Justice held that the rule was admissible under Union law with regard to Article 345 TFEU.[77] According to the ECJ, the interest in excluding private individuals constitutes a 'compelling reason of public interest' and may justify restrictions on fundamental freedoms.[78] The considerations for a national principle of digital sovereignty listed above could constitute compelling reasons of public interest as well. If it is permissible under EU law to exclude private parties from the operation of energy distribution networks completely, a partial exclusion of private parties from state tasks of data processing regarding the involved data and the state tasks in question must be permissible as well.

6.2 GDPR

Private IT service providers will regularly become involved in state tasks as a processor. Article 28 and 32 GDPR define specific requirements for processing data on behalf of a controller which IT service providers need to meet in order to be considered as possible processors. Like the former Data Protection Directive 95/46/EC, the GDPR follows a comprehensive approach.[79] The principle of

---

74 Elke Gurlit, *§ 108 GWB*, in *Beck'scher Vergaberechtskommentar – Zweibändige Ausgabe*, marginal no. 3 (2nd ed., Martin Burgi & Meinrad Dreher eds, C.H. Beck 2018).

75 *See* e.g. Case C-107/98 *Teckal Srl v. Commune di Viano (Teckal)* ECLI:EU:C:1999:562. [1999] ECR I-8121; Case C-26/03 *Stadt Halle v. Recyclingpark Lochau (Stadt Halle e RPL Lochau)* ECLI:EU:C:2005:5 [2005] ECR I-26; for public-public joint ventures: Case C-324/07 *Coditel Brabant v. Commune d'Uccle (Coditel Brabant)* ECLI:EU:C:2008:621 [2008] ECR I-8486.

76 Gregor Kirchhof, *§ 15 Europäische Integration und Privatisierungen, in Verwaltungsrecht der Europäischen Union* 585–618 (2d ed., Jörg Philipp Terhechte ed., Nomos 2019). Thorsten Kingreen, *Art. 345 TFEU*, in *EUV/AEUV*, marginal no. 10 et seq. (5th ed., Christian Calliess & Matthias Ruffert eds, C.H. Beck 2016).

77 Case C-105/12 *Staat der Nederlanden v. Essent NV (Essent* et al.*)* ECLI:EU:C:2013:677.

78 *Ibid.*, para. 49 et seq.

79 Case C-101/01 *Bodil Lindqvist (Lindqvist)* ECLI:EU:C:2003:596 [2003] ECR I-12971, marginal no. 96; cf. also Case C-524/06 *Huber v. Bundesrepublik Deutschland (Huber)* ECLI:EU:C:2008:724 [2008] ECR I-9705 marginal no. 51; Joined Cases C-468/10 and C-469/10 *ASNEF v. Administración del*

digital sovereignty can, however, be understood as an additional requirement by national law for entering into a contract of data processing in terms of Article 28 GDPR. As a consequence, in the cases covered, private IT service providers may not be considered.

Such additional national requirements do not per se contradict the GDPR. As outlined above,[80] pursuant to Article 6(1)(e) GDPR, data processing is lawful, among other things, if it is necessary for the performance of a task which is in public interest or if it is carried out in the exercise of public authority assigned to the person responsible. In such cases, according to Article 6(2,3) GDPR, the national legislator can introduce more specific provisions in order to adapt the provisions of the GDPR. This opening clause intends to enable the Member States to independently implement concrete legal provisions in order to be able to fulfil their own constitutional obligations.[81] Therefore, the principle of digital sovereignty is covered by this provision, too. Article 6(3) sentence 3 GDPR determines various aspects which can be specified by the Member States, whereby the legal nature, legal form or applicable legal regime of the processor and his institution are not mentioned. The enumeration, however, is expressly not to be understood as conclusive. In addition, national law can determine who should be responsible in the sense of data protection law. If this power expressly allows to determine a natural or legal person of private law as responsible, it must also be possible to regulate the group of possible processors.

7 CONCLUSIONS: INTERNALIZING DATA STORAGE

Compared to article-based documents, the management of data with digital tools allows the delocalization and/or the centralization of most of the activities and resources needed for data storage (e.g. data centre).

For example, a single IT platform can be made available to several administrations, in order to offer the same infrastructure to many subjects. This solution can have the advantage of fostering the creation of centres of excellence with the

Estado (ASNEF) ECLI:EU:C:2011:777 [2011] ECR I-12181 marginal no. 28 et seq.; Case C-582/14 *Breyer v. Bundesrepublik Deutschland (Breyer)* ECLI:EU:C:2016:779 marginal no. 57 et seq.; Eugen Ehmann & Martin Selmayr, *Introduction*, in *Datenschutz-Grundverordnung: DS-GVO*, marginal no. 76 (2nd ed., Eugen Ehmann & Martin Selmayr eds, Beck 2018). Peter Schantz, *Art. 1*, in *Datenschutzrecht in Bund und Ländern*, marginal no. 8 (26th ed., Heinrich Amadeus Wolff & Stefan Brink eds, C.H. Beck 2018). Stephan Poetter, *Art. 1*, in *Datenschutz-Grundverordnung: DS-GVO*, marginal no. 24 (Peter Gola ed., C.H. Beck 2018).

[80] Compare *supra* para. 4.

[81] Marion Albers & Raoul-Darius Veit, *Art. 6*, in *Datenschutzrecht in Bund und Ländern*, marginal no. 58 (26th ed., Heinrich Amadeus Wolff & Stefan Brink eds, C.H. Beck 2018). Benedikt Buchner & Thomas Petri, *Art. 6*, in *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG*, marginal no. 92 et seq. (Jürgen Kühling & Benedikt Buchner eds, C.H. Beck 2017).

resources, means and capabilities necessary to ensure greater guarantees in terms of continuity and sustainability of the services to be provided.[82] This can be especially true where a high fragmentation of institutions would make it easier to create one or more delocalized systems serving at once multiple entities.

These advantages have been underlined by the Agency for Digital Italy, according to which cloud computing makes it possible to concentrate complex and costly technologies in large data centres, from which services are provided to citizens, businesses and administrations in an efficient and secure manner, at very low costs. In this way, administrations also drastically reduce the costs of managing IT infrastructures.[83]

However, we have underlined that the choice of the organizational measures to be adopted for data storage should be limited to solutions that ensure that data remains within the public sphere. Nevertheless, it is possible to achieve organizational models that make the most of the advantages offered by information and communication technologies, while entrusting the management of data only to public entities.

An interesting example of this organizational model is offered overseas by the US experience. At the federal level, an entirely public management platform called cloud.gov was introduced in 2015.[84] This service has the specific purpose of allowing federal administrations to use an infrastructure that is always up-to-date and safe to host their technological solutions.[85]

It is also interesting to note that the solution adopted by the US government is a *Platform As A Service*, which means that both the infrastructure, and the basic software required to operate the systems to be installed on the infrastructure itself are provided. The goal is precisely to reduce the skills required by each administration to manage their IT solutions, removing a large part of the infrastructure aspect from the variables that each has to deal with.[86]

The American administration has therefore deemed it appropriate to place at the service of the federal authorities an internal service provided by a single entity

---

82 It is worth pointing out that in the IT industry, due to the continuous and rapid evolution of technologies, systems must be constantly updated and monitored, in order to prevent them from becoming obsolete and for security reasons.

83 *See* the Press Release of 24 May 2016, entitled Consip and AgID: signing the contracts for connectivity and awarded the first two lots of the tender for cloud services.

84 As reported by the website cloud.gov, this is a United States government platform, created and managed by 18F. The latter is part of the General Services Administration, an independent administration established by the Federal Property and Administrative Services Act of 1949, entrusted, among others, with the management and development of the infrastructures necessary to support the other federal administrations (*see* S. 101 et seq.).

85 *See* cloud.gov, where it is stated that 'cloud.gov helps teams build, run, and authorize cloud-ready or legacy government systems quickly and cheaply' (consultation date: Jan. 2019).

86 *See* cloud.gov.

that, according to the European categories of public procurement, belongs to the public sphere. In this way, this solution also excludes the risk that a private entity, if entrusted with supplying the data centre, might have access to a public database and its contents.

A portal such as cloud.gov can reduce the complexity that must be borne by each administration, without at the same time reducing the security of the system as a whole. On the one hand, the risk that a private entity managing the infrastructure may have undue access to the data is excluded. On the other hand, the high specialization of the appointed entity can guarantee high quality standards compared to what every single administration could do.

It can also be noted that the use of the services offered by cloud.gov is left to the free choice of each administration, which can evaluate on a case-by-case basis whether to rely on a central infrastructure, or not. Therefore, the creation of such a subject does not necessarily postulate the prior mandatory identification of the administrations that will have to make use of it, while being able to leave this assessment to the appreciation of the single entities. It is also worth noting that the services offered by cloud.gov are not free,[87] so that this evaluation can be carried out also from a strictly economic point of view.

A similar approach is the one of European institutions, which have recently started an ambitious project to preserve data according to the logic of cloud computing.[88] A particularly interesting aspect of this project is that, also in order to protect the confidentiality and security of data, both internalized solutions and outsourcing solutions have been implemented.[89] This is precisely in order to overcome the concerns that have been outlined above regarding the risks of entrusting a private operator with the data centre hosting public administration databases.[90]

---

87 In Jan. 2019 the costs of the service are identified, https://cloud.gov/pricing/.

88 *See* the procedure on 27 Dec. 2014, DIGIT/R2/PO/2014/043 Cloud Services (CLOUD I), https://etendering.ted.europa.eu/cft/cft-display.html?cftId=684.

89 According to the provisions of the call, the tender was divided into three lots: (1) 'Private Cloud IaaS (Infrastructure as a Service)': 'services to be procured can be understood as an extension to the existing European Union Institutions (EUIs) data centres. It is intended to host information systems which risk profile is considered low to moderate in terms of confidentiality, criticity and personal data protection'; (2) 'Public Cloud IaaS (Infrastructure as a Service)': 'services to be procured intends to host production and non-production environments for information systems which risk profile is considered low in terms of confidentiality, criticity and personal data protection'; (3) 'Public Cloud PaaS (Platform as a Service)': 'series of Managed Services identified of value, partially or entirely managed by the provider' (tender documentation available to the address, https://etendering.ted.europa.eu/cft/cft-documents.html?cftId=684).

90 At this regard it was stressed that the EU initiative to create a Cloud infrastructure for European institutions has not only technological, but also political relevance, *see* Giancarlo Vilella, *Introduzione alla E-Democracy* (Pendragon 2017).

In conclusion, we have shown how the critical nature of the data held by public administrations, as well as the dangers inherent in relying on private structures, favour internalized solutions for the storage phase of the data supply chain. Moreover, the US and European examples confirm that it is possible to appoint entities with proper technological competence for the internalized such activities, without therefore necessarily changing the organizational structures of the institutions involved.