European Review of Digital Administration & Law - Erdal
2024, Volume 5, Issue 1, pp. 225-236
ISSN 2724-5969 – ISBN 979-12-218-1507-8 – DOI 10.53136/97912218150783 17

*Exploring the Potential of the Danish Principle of Administrative Law by Design: A Possible Pathway for Avoiding Mistrust in Public IT**

Hanne Marie Motzfeldt
(Professor in Public Law and Digitalisation, PhD, Faculty of Law, University of Copenhagen)

Johan Næser
(Assistant Professor, Department of Law, Faculty of Business and Social Science, Aarhus University)

ABSTRACT The article explores the sharing and reuse of objective and verifiable information in the digitized public administration. The Danish principle of administrative law by design is being introduced. This principle may ensure a greater interaction between national administrative law and EU law, especially the General Data Protection Regulation (GDPR), and be a possible pathway for avoiding mistrust in public IT systems.

KEYWORDS: Administrative law by design – GDPR – Data sharing – Public IT systems

1. *Introduction*

The reuse of information (data sharing) is an essential prerequisite for a partially or fully automated administration, meeting the need for efficiency in the large public administrations of the European welfare states. Data sharing within the digitalised public sectors in the EU has been promoted for decades.[1] Consequently, the once-collected information is reused in varying administrative contexts and by different administrative bodies, at least in countries with highly digitized public sectors.

However, one of the lessons learned from some recent European cases is that too much trust in data circling the digitized public administrations might be unjustified. Extensive data sharing entails a risk that incorrect or inadequate (deficient) information spreads and negatively affects the outcome of decisions directed at citizens or other actions taken by public bodies. Three striking examples from different countries can be mentioned. In the British post office scandal, many people were wrongly prosecuted after faulty software indicated money was missing from their Post Office branch accounts. Thus, more than 900 sub-postmasters were prosecuted for theft and false accounting because of incorrect information from a computer system called Horizon.[2] In the Dutch case of System Risk Indication (the so-called SyRI-case), a digital system was matching several public data sources in order to detect an increased risk at social security fraud. However, a Dutch court found the digital system to breach human rights, i.e. the right to respect for private life and the protection of personal data.[3] In the Danish

* Article submitted to double-blind peer review.
This article is a revised version of H.M. Motzfeldt and J. Næser, *Datakvalitet i den forbundne digitale forvaltning*, in R.G. Nielsen (ed.), *Hyldestskrift til Poul Andersen*, Copenhagen, Djøf Publiching, 2024.

[1] Visions and initiatives for data sharing and a so called "once-only" principle, mening citizens only once have to provide information to public administrations, have been key elements of the recent National Danish public digitalisation strategies. See for instance the Danish Goverment, Local Goverment Denmark and Danish Regions, *A Stronger and Safer Digital Society,* 2020, especially 7-10 and 25-28.

[2] BBC, *Post Office Horizon scandal: Why hundreds were wrongly prosecuted*, 2024.

[3] S. Bekker, *Fundamental Rights in Digital Welfare States: The Case of SyRI in the Netherlands*, in O. Spijkers et al. (ed.), *Netherlands yearbook of international law*, The Hague, T.M.C. Asser Press, 2019, 290 and 297-298.

case of the development and use of a new IT system for automated debt collection (the so-called EFI-case), the system was subsequently closed down (suspended) partly due to insufficient quality of data used in the IT system.[4]

In the public administration, such cases not only cause concerns of harming citizens, for example, by depriving them of rights or benefits. The use of incorrect or inadequate data can also lead to decisions or actions not intended by the legislators, which may, in principle, endanger the balance between the executive and legislative power. Further, such data may provide some citizens with unjustified and arbitrary advantages or benefits, thereby undermining the principle of equality and trust in the objectivity of the public sector (although erroneous data could be an advantage for the specifically involved citizens in a given situation).

> A rather entertaining illustration of incorrect data leading to arbitrary advantages in Denmark was covered by national media in 2019. Here, several municipalities had initiated maintenance of private bridges due to data incorrectly showing that the bridges in question were publicly owned. One of the cases involved two brothers, Egon and Gerhart Rasmussen, who owned a private bridge on their farming land. According to media coverage, the brothers stated: "[t]hese people from Aabenraa Municipality are really nice", as the brothers realised that Aabenraa Municipality had spent DKK 700,000 on a new bridge to replace the brothers' old bridge".[5]

In light of the ever-increasing digitalisation of the public sectors in Europe, the complications caused by data reuse have become of significant practical interest. In the following, we will focus on an easily overlooked theme: the sharing and reuse of objective and verifiable information. In other words, it is not a subjective assessment, such as profiles generated by AI, but simply information that can be verified if counted, measured, weighed, or otherwise documented, and no subjective elements are involved.

The legal implications of incorrect objective and verifiable information might seem simple and the theme therefore of no theoretical interest. In terms of accountability, at least in Denmark, there is no doubt that a competent public body would be responsible for ensuring that such objective information represented reality when used as the basis for a decision or in the performance of other administrative activities in the analogue administration. However, in the (newer) reality of digital administration, the burden of controlling the vast amount of data interferes with realities (resources) and the ideals of smooth, automated processes. Today, control of all data used in all contexts in the public sector can seem highly difficult, if not unrealistic. As a consequence, new regulatory approaches are needed. Danish administrative law has developed important principles through the Parliamentary ombudsman case law that may be able to prevent a future Danish Post office scandal. As these principles simultaneously ensure a somewhat harmonic interaction between national administrative law and EU law, especially the General Data Protection Regulation (GDPR), this development may inspire other EU member states – and thus be of theoretical interest.[6]

In the following section 2, the development of the digital infrastructure for data sharing in the Danish public administration is outlined. Section 3 provides, first, a short overview of the relevant principles of Danish administrative law, as these were developed for analogue administration, and second, the developments adapting the general legal framework to the digitized administration until 2021. Third, an analysis of the new case law from 2022, which relates to the theme of data accuracy and clarity of duties and responsibilities within the chains of data flows in the digitized Danish administration. In section 4, we turn towards the requirement of personal data accuracy and integrity in EU

[4] See Bill no. 232 of 5 May 2021 on a bill to amend, inter alia, the debt collection Act, section 1 of the general comments to the bill. The EFI case has being analysed severeal places in the Danish legal literature. See for instance H.M. Motzfeldt, *EFI og rammerne for udvikling af digital forvaltning*, in N.S. Clausen (ed.), *Festskrift til Sten Schaumburg-Müller*, Copenaghen, Djøf Publishing, 2016.

[5] See the Danish newspapers Landbrugsavisen, *Another bridge blunder: Municiplaity repaired farmers bridge by mistake (Endnu en bro-bommert: Kommune renoverede ved en fejl landmands bro),* 2019, and Jydske Vestkysten, *Municipality sendt DKK 700.000 on private bridge: It was a mistake (Kommune har brugt 700.000 kroner på privat bro: Det var en fejl)*, 2019.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

data protection regulation in order to use the next section 5 to describe how national Danish digital administrative law and EU law mutually support each other by embracing similar proactive and systemic approaches.

2. *The infrastructure for dataflows in the Danish digital administration*

As the digitisation of the Danish public administration may have begun with the development and use of simple standalone systems as early as the middle of the last century, a trend towards more and more sophisticated process-steering and process-supporting systems began in the 2000s. As this development caused an increasing need for data to feed these systems, it became apparent that there was potential for significant efficiency improvements by intensifying data sharing across the public administration. This potential was initially realised via connecting systems bilaterally in order to exchange data through these connections (integrations). This 'bilateral' approach resulted in a somewhat overwhelming cobweb of interconnected systems as most systems had to be connected to more than one other system.[7]

The above-described and somewhat chaotic model for a data-sharing structure still exists in the Danish administration. However, the lack of transparency and the many integrations, which are maintenance-intensive and lack robustness, have led to more strategic and systematised approaches to data sharing. In the recent decade, many sector-specific databases (registries or data warehouses) have been established. In recent years, data-sharing layers have been added to decrease the need to connect systems bilaterally or copy data via shared databases.

As far as databases are concerned, large cross-sectional registers have always been an essential part of the digital infrastructure in Denmark. The cross-sectional registers contain primary data used in almost all areas of administration, e.g. the Danish Civil Registration System (CPR) with basic information on citizens (national identification number, date of birth, place of residence, family relations, etc.) and the Danish Building and Housing Register (BBR) with basic information on parcels and real estate (localisation, permits, potential pollution of the soil, restrictions on use, the status of water and heating infrastructure etc.). The newer, sector-specific databases are, for example, the so-called CRAM register, which holds labour market data from the Employment Service administration, and the Shared Medicine Card, see regarding the Shared Medicine Card in section 4. These sector-specific databases meet the need for data sharing by connecting different systems to the database, feeding and retrieving data to and from the databases. In other words, the bilateral filtered skein of systems is avoided. On the other hand, many systems need to be connected to these databases and data need to be copied into the databases. This has led to the development of the newer distributing data-sharing layers. Distributing data-sharing layers are systems specifically designed to distribute data to and from different systems without duplicating the dataset. An example of such a system is the Data Distributor, maintained by the Danish Agency for Data Supply and Infrastructure (SDFI), which distributes data about persons, companies, addresses, real estate, geographical data, and maps. Another example is the Service Platform through which the Danish Municipality IT company, KOMBIT, distributes data and functionalities to the municipalities.

Through the described digital infrastructure, vast amounts of data are distributed from and to all corners of the Danish administration to be used and reused for different administrative activities. This development towards a data-driven public sector caused a development within administrative law in 2022, intending to counteract the risk of spreading and using incorrect data and, thereby, wrongful IT administration (see further in section 3.3).

3. *The principle of administrative law by design and data sharing in Danish administrative law*

3.1. *Introduction*

As in most EU member states, the Danish public bodies are bound by the investigation principle.[8] This fundamental principle

[7] Challenges with regard to interconnected IT systems were the very theme of two recent reports from the Danish Parliamentary Ombudsman, see section 3.3. below.

[8] On the Danish investigation principle, see F. Waage, *General Principles of Danish administrative law*, Copenhagen, Hans Reitzels Publiching, 2022, 371-372.

developed over centuries in Denmark, mainly for the analogue administration, and implies that public bodies are obliged to provide the relevant and necessary information about cases at hand before decisions or actions are taken. Even though the procedures vary within the different administrative areas, a common denominator is that the required information is usually gathered through mutual cooperation between public bodies and with private actors' assistance. It has traditionally been assumed that information collected from other public authorities has a high degree of reliability (accuracy), and this presumption reduces the obligation of the receiving public bodies to control such information. The opposite applies to information gathered from private actors, which consequently needs to be controlled before being used as a basis in a case.

> The abovementioned presumption has impacted Danish administrative law at all levels. It is, for example, reflected in the understanding of the exception to the duty of consultation of concerned parties in section 19(2)(1) of the Danish Public Administration Act.[9] This provision allows public bodies to abstain from consultation if the information at hand is reliable. According to the legislative preparatory documents, this includes "information from the tax authorities about taxable income, social income and in general information which, because it originates from a public body, has a similar authentic character".[10]

The background to the Danish presumption of the correctness and accuracy of public stored data is lost in the legislative history, case law and legal literature of the past, where the presumption functioned in a different administrative reality than today's systematised data gathering and sharing. It is thus an important question under which circumstances and proactive measures this presumption – and the resource-saving effect hereof – can be maintained in the present digital administration without causing systematic wrongful decisions due to incorrect data, like for instance in the British post-scandal. Here, the recent developments within Danish administrative law have provided a potential solution. This development must, however, be seen in the background of the previous case-by-case development, going back to the early digitalisation of the 1990s.

3.2. *The Danish Principle of Administrative Law by Design*

In Denmark, case law from the Parliamentary Ombudsman has long followed the development of the digitalised public administration, utilising the in-build dynamic in Danish administrative law and thereby developing new principles of administrative law.[11] So far, two starting points have dominated the approach in the Ombudsman's case law. The first is that the rules and principles of administrative law apply when the administration is analogue as well as when it is supported or managed digitally.[12] In other words, Danish administrative law is regarded as technology-neutral unless otherwise clearly stated in statutory regulation (specific legislative acts). The second starting point has been that every public authority is responsible for ensuring that its organisation and procedures (manual or in-build in it-systems) within its designated area are designed to support compliance with applicable regulations and principles of good administration.[13]

Danish case law has utilised the above in a proactive approach to the development, updating, implementation and use of it-systems. In brief, the Danish Parliamentary Ombudsman has stated that it is "a fundamental requirement that public IT systems are designed to support the correct application of the relevant regulation - including the statutory and non-statutory rules and principles of administrative law", which is best ensured by early identification and

[9] Consolidated Act no. 433 of 22 April 2014 on the Public Administration Act.

[10] See Bill no. 4 of 2 October 1985 on the Danish Public Administration Act, paragraph 19 of the specific comments to the bill. See also the Guide no. 11740 of 4 December 1986 to the Public Administration Act, section 112.

[11] About the underlying drivers of the development of the principle of administrative law and the requirement of a good impact assessment in Denmark, see H.M. Motzfeldt, *The Danish Principle of Administrative Law by Design*, in *European Public Law*, vol. 23, no. 4, 2017, 739-754.

[12] This can be seen for the first time in FOB 1997.198 and has since then been consistently maintained in the Parlimentary ombudmand case law.

[13] The underlying Ombudsman's case law supporting this second starting point is analyzed in H.M. Motzfeldt and A.T. Abkenar, *Digital forvaltning – udvikling af sagsbehandlende løsninger*, Copenhagen, Djøf Publishing, 2019; H.M. Motzfeldt, *Tilsyn med sagsbehandlende it-løsninger: om den digitale forvaltnings hyldevarer*, in *Nordisk Administrativt tidsskrift*, no. 3, 2016, and H.M. Motzfeldt, *Den danske ombudsmands krav om værdibaseret design af den digitale forvaltning*, in *Nordisk Administrativt Tidsskrift*, no. 3, 2015.

incorporation of the regulation in question. "Therefore, the development (and updating) of IT systems for the Danish public sector requires, among other things, a mapping of the types of cases and processes that a new system (or an update) will affect, as well as the procedural and material rules that apply to the said cases and processes. According to Danish Administrative law, this mapping is to be initiated from the very beginning of the development or updating process and utilised when deciding how a new system is to be designed, as the chosen design has to support compliance with the mapped regulation. Furthermore, it has – also since 2014 – been a prerequisite that the relevant legal expertise be available in all important phases of a development or updating process. A requirement that thorough testing is performed before a system is put into use has gradually been added after 2014.[14]

Regarding data gathering, data sharing and the investigation principle, the starting point has been the technology neutrality of Danish Administrative law. Consequently, it has been the duty of any Danish public body to gather information to the extent necessary for taking a decision on a qualified basis, i.e. take the initiative to obtain the information that is typically relevant in the type of case at hand and, if necessary, check the accuracy of this information.[15] Further, as Danish administrative law is technology-neutral, public bodies are still allowed to operate with the traditional presumption that information from other public bodies, in general, is reliable. In other words, if nothing else is indicated, data from private actors are to be controlled, and data from public bodies can be regarded as high quality.

> Statutory reporting obligations for private actors may and may not affect the above. As a start, an interpretation of the regulation laying down the reporting obligations must be decisive on whether such obligations entail a presumption of correctness and whether administrative bodies can rely on this presumption besides the body to which the information must be reported. If nothing can be deduced from the relevant legislation, it must be taken into account that incorrect or incomplete data can be reported due to simple negligence and that errors and omissions can arise due to the design of systems or the integration between them. As such erroneous data can be shared before an affected party is given the opportunity to protest, the starting point must be that the establishment of reporting obligations does not affect the above starting points, even when penalties have been established for intentional or grossly negligent incorrect reports.

In reality, the presumption for reliable data within the public sector only has ground if data previously originating from private actors have been controlled and *if* malfunctions in the different, integrated system have not corrupted the data. If, on the other hand, one of the data-sharing systems has been flawed and thereby corrupted the data or *if* the information was obtained from parties or other private actors without the collecting – and later sharing – public body having carried out any quality control, the technology of this presumption embedded in the investigation principle naturally entails a risk of a Danish Post office scandal. It is unclear, but most weigh in favour of the presumption of correctness to waive in some scenarios. If there are indications in a specific case that the information obtained is incorrect, the public body in question must investigate this further before taking a decision or setting an action in motion, regardless of the questionable information originating from another public body. Indications may, among other things, be inquiries or consultation responses from involved parties or other data sources indicating a discrepancy. This approach can, for example, be seen in a decision from the Danish Environment and Food Appeal Board in 2022. The background of the appeal was the Danish Agricultural Agency´s use of incorrect information originating from a municipality in a refusal of farmland subsidies. The municipality, Syddjurs Municipality, had mistakenly reported an area as protected under Section 3 of the Danish Nature Protection Act via the databases in the Danish Environment Portal (a portal displaying information from sector-specific databases in Danish nature and environmental administration). This erroneous information had been copied to the Danish Agricultural Agency's Internet Land Map (IMK).[16] Even

[14] Cf. FOB 2023-7 on the police weapons register, FOB 2023-15 on the Municipalities' Benefits System (KY) and FOB 2023-3 on one of the Danish Agency for Labor Market and Recruitment's (SIRI) self-service systems.

[15] N. Fenger (ed.), *Forvaltningsret*, Copenhagen, Djøf Publishing, 2018, 489 ff.

[16] Similar themes are commented in MRF 2023.91 regarding the Environmental and Food Board of Appeal's decision of 29 March 2023, j.nr. 23/01950,

though the complainant had made the Danish Agricultural Agency aware of the incorrect information, the Agency based its decision on the so-called official information from the IMK. In response to the complainant's objections, the Danish Agricultural Agency replied *that* at the relevant time, the area was registered as protected in the Danish Environmental Portal, *that* the incorrect registration was a matter to be handled between the complainant and Syddjurs Municipality, and *that* the IMK was only updated once a year. Based on this, the Agency maintained that the official registration - and not the actual status of the area - was decisive. The Environment and Food Appeals Board initially stated that according to the investigation principle: "a public authority has a duty to gather the relevant and necessary information before a decision in a case is taken [and this] obliges the authority to actively ensure that all relevant and necessary information is collected *and* controlled". Accordingly, the Board overruled the Danish Agricultural Agency and returned the case for reconsideration on the grounds that the investigation principle had not been complied with.[17]

In addition, the presumption of accuracy (reliability) of data originating from other public bodies will probably have to be reconsidered *if* there are clear indications or even knowledge of not negligible percentages of errors in a data set. This may be the background for a newer legislative theme in Denmark. It can be observed that public bodies increasingly wish for statutory derogations, ensuring they are not obliged to control shared and reused data. One example can be found in the preparatory work for the amendment to the Danish Pension Act, which established a new pension in Denmark named Early Pension, which, from the beginning, was intended to be managed (mainly) fully automatically. In their consultation response during the legislative process, the designated administrative organisations, ATP and Udbetaling Danmark, suggested that it should be clearly stated that "Udbetaling Danmark uses the information from the external registers [databases] as the basis for the administration without control hereof".[18] Another example can be seen in the Danish Real Estate Assessment Act, stating in the preparatory documents that unless there is obviously incorrect data in a specific case, information from sources within the public administration will be considered "correct and up-to-date and generally reliable". In relation to incorrect data in the BBR register, which is mentioned above in section 2, it is stated explicitly that affected citizens are to contact the public bodies responsible for reporting information to the BBR if corrections are required.[19]

> The Danish Real Estate Assessment system was released for partial use in 2024, and caused considerable political and legal attention. Among others, some of the assessments were flawed to an extent that clearly exceeded any discretionary margin. The Danish tax minister stated that these assessments were "completely on the moon ". In FOB 2024-10, the Danish Parliamentary Ombudsman published his opinion that the implementation of the system before it was able to better generate and administer fair assessments had damaged the Danish population's trust in the tax authorities.

As mentioned in section 1, it is, on the one hand, obviously problematic if the public administration uses incorrect information as a basis for decisions and actions, regardless of whether these decisions and actual actions can be regarded as in favour of a specific citizen or not. On the other hand, especially in areas of mass administration, control of all data will

where it is stated that if there is an error registration in IMK, it is difficult to justify a cross-compliance sanction.

[17] See the Environment and Food Board of Appeal's decision of 16 February 2022, *Annulment and referral in case of rejection of application for organic area subsidy 2021* in *Syddjurs Municipality, Environment and Food Board of Appeal file number 22/00687* (Miljø og Fødevareklagenævnets afgørelse af 16. februar 2022, Ophævelse og hjemvisning i sag om afslag på ansøgning om tilsagn om økologisk arealtilskud 2021 i Syddjurs Kommune, Miljø og Fødevareklagenævnets journalnummer 22/00687).

[18] Collected consultation responses to bill no. 104 of 18 November 2020 amending the Social Pension Act and various other acts (Introduction of the right to Early Pension), 14.

[19] Consolidated Act no. 1449 of 1 October 2020 as amended and bill no. 211 of 3 May 2017 on the Real Estate Assessment Act, section 2.13.2.1. Regarding the so-called preliminary assessments, it is clear from the preparatory works of the Real Estate Assessment Act that incorrect or incomplete data may be used to form the preliminary assessments in order to automate the administration, see Bill no. 114 of 26 April 2023 amending the Withholding Tax Act, the Municipal Income Tax Act, the Real Estate Assessment Act and various other acts, section 3.4.2 (the Ministry of Taxation's considerations and the proposed scheme).

be very resource-intensive and thus not realistic in the large administrations in the welfare states. In other words, a need for alternative approaches to strengthen the efforts to ensure the quality of data shared and reused in public administration increases in line with digitalisation and the need for data sharing.

3.3. *Recent case law in Denmark*

In two recent reports, FOB 2022-11 and FOB 2022-12, the Danish Parliamentary Ombudsman has taken the first steps towards reconciling the underlying values and ideals of the investigation principle with the realities of the digitized administration resources and the newer ideals of automated processes. These steps were taken in two cases investigating the development of a system named Deleøkonomisk Indberetningsløsning (which can be translated into 'The reporting portal for income from shared economy activities')[20] and the update process of an ESDH system (electronic case and document management system) within the Danish tax administration, both systems developed by a designated body within the Danish Ministery of Taxing.

The purpose of the reporting portal for income from shared economy activities is, primarily, that companies subject to a Danish statutory reporting obligation regarding profit from shared economy activities report the profit (income) via the system.[21] Secondly, the system aim to forward the collected data to the Danish eIncome register.[22] From the eIncome register, the information is reused by different public bodies for varying purposes.[23] For example, Udbetaling Danmark's task to taxprofits and calculate and control welfare benefits .

Certain platform operators are required to report users' income under section 43 of the Danish Tax Reporting Act and section 3(1)(2) of the Danish Income Register Act. This obligation is implemented via an Executive Order on Tax Reporting, etc. eIncome is a database (register) administered by the Danish Tax Administration, which is the data controller.

The Danish Parliamentary Ombudsman chose to investigate the development of the reporting portal for income from shared economy activities as part of an effort to generally strengthen Danish tax administration's compliance in relation to public digitalisation. The Ombudsman chose to observe the procedures during the development of the IT system. i.e. at an earlier stage than usual (preventive approach), as the Danish Parliamentary Ombudsman normally only goes into a case when it has been finally concluded by the authority.[24] In the later report, the Ombudsman emphasised that this approach aimed to "uncover whether more general or systemic themes can be derived from the development of the IT system, which the authorities should be aware of".

Concerning data sharing, it is *firstly* of interest that the Parliamentary Ombudsman, in his report, highlighted the fact that Danish public IT systems interact with other systems, and such interaction can be within the same organisation and/or extend to several public organisations. Therefore, the Ombudsman stated that a public body developing a new system cannot limit the mapping and investigations described above in section 3.2

[20] The sharing economy reporting solution went live at the beginning of 2021 with a deadline of 20 January 2022 for reporting information on rental income from the rental of year-round homes, holiday homes, cars, yachts and caravans, etc. for the 2021 income year, see access to the system via https://info.skat.dk /data.aspx?oid=54165, last accessed on 27 July 2024.

[21] Companies operating sharing-economy platforms such as Airbnb and GoMore or rental agencies. The report from the Parlimantary ombudsman is also discussed in L. Skriver, *Masseforvaltning i et forvaltningsretligt perspektiv - tredjepartsdata i skatteretten*, Copenhagen, Djøf Publishing, 2023, 310 ff.

[22] The Income Register Act stipulates a number of reporting obligations that include salary income, employee benefits, grants and transfer income, cf. section 3(1) of the Income Register Act. See al so Skatt's legal guidance 2024-1, section A.B.1.1.3.4.1 Reporting to eIncome, available at https://info. skat.dk/data.aspx?oid=2284512, last accessed on 27 July 2024.

[23] See Bill no. 102 of 14 November 2018 on a bill to amend the Real Estate Assessment Act, the Property Value Tax Act, the Income Register Act, the Personal Tax Act and the Tax Reporting Act, section 2.3.2 of the general comments to the bill, and the comments to section 3 of the bill amending section 3(1) and section 4(1) of the Income Register Act.

[24] This new angle on monitoring the authorities' digital solutions is described in *The Annual report from the Danish Parliamentary Ombudsman,* 2021, 5-6. In this annual report, the following is, inter alia, stated in relation to monitoring IT systems: "We will attempt to enter the process relatively early – meaning already at the development stage of the IT systems – in order to see if we can play a part in the authorities preventing and avoiding flaws rather than just wait for the damage to be done and then react to complaints about fully developed systems".

to the specific, new system. The public body is obliged to consider the context in which the system is later to be used and expand the mapping, if relevant. In other words, the public body (proactively) has to determine whether the purpose of a new system is to receive and/or disseminate data, which will be used as the basis for decisions in the developing body's other systems or in other organisations' systems. If this is the case, the developing body is to enter into dialogue and coordination with those responsible for these other systems and/or the authorities to receive data. In this connection, the public bodies are to map where and how the data flows through the different systems –including in which IT systems and under the responsibility of which organisations – compliance with the requirements of administrative law will be supported.

Secondly, it is striking that the report from the Danish Parliamentary Ombudsman on the development of the reporting portal for income from shared economy activities emphasises that: "such mapping and determination of responsibilities and roles in relation to the requirements of administrative law, etc. [are] of great importance in ensuring that these legal requirements are ultimately complied with. Such considerations may also be of importance even when a system only is to receive and transmit information later to constitute the basis for decisions taken in or via support of other systems, as this may be of relevance to fulfil such a receiving and transmitting systems' purpose and ensure a solid basis for the subsequent use of the data". In other words, the Danish Ombudsman addressed the very theme of this article, namely that unclear responsibilities and roles in the digitally connected public administration increase the risk of insufficient data quality control and, thereby, unnoticed spreading incorrect data and their use in various administrative contexts.

FOB 2022-11 on the reporting portal for income from shared economy activities was published simultaneously with FOB 2022-12 on the upgrade of the Tax Administration's ESDH system. In the report on the upgrade of the Tax Administration's ESDH system, the Danish Parliamentary Ombudsman first and foremost stated that the requirements for mapping, ensuring an adequate design and testing apply to upgrades as well as to the development of new systems. How comprehensive such processes are to be will depend on "the nature and scope of the upgrade, including the importance of the upgrade for the system's compliance with administrative law and citizens rights". In the report, it is mentioned that it is to be investigated as a part of an upgrade whether there are existing problems in relation to legal compliance, whether new legislation, case law or changing conditions in the area are relevant, and whether the upgrade may have unintended consequences in other parts of the system in question *or* for the interaction with other systems. Further, FOB 2022-12 follows up on previous case law and clearly states that "the public bodies responsible for the development or upgrade of an IT system – after the system has been put into operation – are to follow up and examine whether the system supports compliance with relevant legislation as intended. Such follow-up includes investigating whether existing compliance issues have been resolved as intended or whether new problems of this nature have arisen. Finally, the Danish ombudsman repeated his statements from the report on the reporting portal for income from shared economy activities. According to the Ombudsman, both the upgrading and follow-up are thus to take place in dialogue and cooperation between the public bodies involved in order to ensure that potential issues are identified and handled.

As can be read between the lines, the Danish Parliamentary Ombudsman did not specify at which stage of a data flow public bodies are to control the accuracy of gathered data. However, the institution has now challenged the Danish public administration to take a proactive approach by demanding a well-researched assessment of potential risks in advance and coordination with the public organisations that can be foreseen to receive and use the gathered data. The reports thereby indicate that the Danish Parliamentary Ombudsman's continuous search "in the legal toolbox for approaches able to function meaningfully in the new technological framework "in relation to the investigation principle ended in a focus on proactive measures to ensure a sound design of the lifecycle of data flows.[25] This will, of course,

[25] N. Fenger, *Ombudsmanden – et værn for borgernes retssikkerhed*, UfR 2020B.37, in *Ugeskrift for Retsvæsen (Journal)*, 2020, 42.

in itself be a burden on the administration. However, the similarities with the GDPR approach might lessen the burden of these mandatory proactive measures; see section 4 below about the GDPR approach and its impact on the data flows in the digitalised administration in Denmark.

4. *Accuracy and integrity of personal data*

4.1. *Introduction*

In relation to data accuracy and the design of data-sharing systems in the public sectors within the EU, provisions in GDPR constitute a fine-tuned regulatory framework.[26]

Article 5(1)(d) of the GDPR states that personal data must be accurate when processed and, where necessary, kept up to date. Further, every reasonable step must be taken to ensure that inaccurate data be erased or rectified without delay. Article 5(1)(d) of the GDPR thus contains obligations to verify as well as to update where updating makes sense in light of the purpose of the processing. This obligation is imposed on the organisation to determine the purposes and means of data processing (the data controller). The burden hereof cannot be placed on the data subjects by relying on them to invoke their right to corrections in accordance with article 16 of the GDPR as such a scenario will only ensure accuracy for the personal data related to data subjects, invoking their right to correction.[27] This also applies to collection, systematisation, storage and sharing of data for the purpose of using them as a (later) basis for decisions or actions in the public sector.[28]

What constitutes reasonable steps to verify the accuracy of personal data is determined in light of the purpose of the GDPR and the principle of accountability, expressed in Articles 5(2) and 24 of the GDPR. The purpose of the GDPR is to promote a single digital market with a high level of protection of citizens' rights, particularly the right to the protection of personal data, cf. article 1(1) and (3) of the GDPR. Thus, the focus is on the data subjects and the protection of their interests. Further, to promote compliance, article 5(2) on accountability states that the controller (for each step in a processing chain) must be able to demonstrate that the processing complies with the principle of accuracy. This obligation interacts with Article 24 of the GDPR. Article 24 requires that collection and reuse (processing) of personal data only takes place where the risks arising from the data processing have been identified and assessed. In other words, a risk assessment must be carried out, and the risks that the processing poses to the data subjects must be identified. Based on these risks and the assessment thereof, relevant measures to ensure accuracy must be identified and implemented effectively, cf. also Article 25(1) and (2) of the GDPR on data protection by design and default.[29] Should it, subsequently, become necessary, e.g. due to data subjects' frequent justified requests for correction under Article 16 of the Regulation, a reassessment after Article 24 must be carried out.

As noted above, the data-protection risk assessment must, among other things, be utilised to determine which measures are to be implemented when collecting and sharing personal data. Determining which measures are appropriate for a specific case of processing depends on which manual procedures and technical solutions are best suited to mitigate the risks to data subjects of processing inaccurate data. The extent and intensity of the measures to be implemented by the controller will thus vary from processing scenario to processing scenario. The more negative impact the use of data may have on assessments, decisions and actions related to the data subject, the more extensive will be the measures to implement. Typically, the amount of data, the nature of processing and the reliability of the data will be of significance.[30] However, the importance of citizens and others being able to trust the information used by public authorities can be a relevant factor as well.

The overlapping requirement laid down in Articles 5(1)(f) and 32(1)(b) is that data

[26] See Articles 5(1)(d), 5(2), and 24 overlapping with the provisions in Article 5(1)(f) and Article 32(1)(b).

[27] This also follows from case law from the Danish Data Protection Agency. See case no. 2018-31-0147, *Alvorlig kritik og påbud til Rejsekort A/S*.

[28] The data subject's right to rectification of inaccurate data is recognised at the treaty level in Article 8(2), second sentence, of the Charter of Fundamental Rights of the European Union.

[29] See also European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* Version 2.0, 2020, 6.

[30] These elements can also be derived from the Danish Data Protection Agency's case law. See for instance case no. 2008-313-0113, *En kommunes ajourføring af adresseoplysninger,* and case no. 2019-819-0003, *Rigspolitiets behandling af teledataoplysninger*.

controllers (and processors) must establish adequate safeguards to ensure that the integrity of personal data is not compromised. This also applies to processing carried out for the purpose of data sharing. In line with this, Article 32(1) of the GDPR states that (all) data controllers must carry out (1) a (security) risk assessment and assess the security risks inherent in the data processing. Based on this risk assessment, the controller must then (2) identify the appropriate technical and organisational measures to protect data subjects against the identified security risks. Furthermore, (3) these measures must be effectively implemented, and the risk and measures must (4) be reassessed and modified where appropriate With regard to the connection to Article 5(1)(d) of the GDPR, the requirements under Article 32 vary according to the risk posed to data subjects by the processing in question. The decisive factor is thus to identify and prevent potential negative consequences for data subjects in the event of a security breach in the form of corruption or loss of information related to them. This can be seen, among other things, in the Danish cases on the Health Platform and the Shared Medical Card from 2022, which we will elaborate on in the following section.

4.2. *The Shared Medicin Card and the Health Platform*

The Shared Medicine Card is operated by the Danish Health Data Authority. The system is designed to provide continuously updated information about medicine, prescriptions, vaccinations, etc., to health practitioners and employees at hospitals, municipalities, and private healthcare clinics. These healthcare practitioners provide and retrieve the data for the system via their organisation's IT systems, which have been connected through various integrations to the Shared Medicine Card.

The Health Platform is an IT system used by Region Zealand and the Capital Region of Denmark, the two authorities on the island of Zeeland (Sjælland) responsible for providing primary healthcare, since the spring of 2016. The Health Platform connects a wide range of the region's IT systems. It has process-supporting and process-controlling (automating) functionalities in relation to several functions, including medication, documentation, surgery booking and ordering laboratory tests. The Health Platform is one of the systems connected to the Shared Medicine Card. Data from the Health Platform are transferred to the Shared Medicine Card via integration applications and the other way around.

On August 10, 2020, July 8, 2021, and August 13, 2021, the Danish Health Data Authority notified the Danish Data Protection Agency that there had been a personal data breach in the form of damages to the integrity of personal data in the Shared Medication Card (incorrect data).[31] In short, over 5,000 prescriptions were mistakenly changed in connection with an update of the Healthcare Platform, leading to flaws in the system. Afterwards, these were automatically transferred to the Shared Medication Card via the integration applications. In addition, the removal of end dates for 267 treatments in the Shared Medication Card had not been transferred to the Health Platform as the integration system had experienced flaws as well.

> In the decisions that followed the investigation of the personal data breaches, the Danish Data Protection Agency initially stated that the Capital Region of Denmark was the data controller for the processing of data in the Healthcare Platform *and* the applications connected to the Healthcare Platform, including the integration providing input to the Shared Medical Card. Conversely, the Danish Health Data Authority was the data controller for processing data in the Shared Medical Card *and* the applications connected to the Shared Medical Card. The data processed via the integrations was, in other words, under the Danish Health Data Authority, even though changes could be made by others (specifically the Capital Region of Denmark).

The Danish Data Protection Agency highlighted that the Capital Region of Denmark's risk assessment should have mapped the data processing in the region's system (the Health Platform) and the integrations and dependencies with other IT systems (the Shared Medical Card). The Danish Health Data Authority, in turn, was obliged (as part of this organisation's risk assessment) to map all integrations between the Shared Medical Card and the sources and recipient systems. The Danish Data Protection Agency emphasized that the Danish Health Data Authority's mapping should have

[31] The relevant case law from the Danish Data Protection Agency is, inter alia, case no. 2020-442-8862, *Alvorlig kritik, påbud og advarsel til Region Hovedstaden efter to sikkerhedsbrud*.

covered not only the technical aspects and the ongoing data flows, but also clarified what actors were responsible the data processing. In other words, in data-protection risk assessments, data controllers involved in data sharing are to produce an overview of 1) their own systems, 2) the integration applications to other actors' systems and 3) the responsibilities and roles of each controller in the sharing of data.

With regard to measures taken to ensure data accuracy and integrity, a number of minimum requirements under data-protection law were clarified in the cases related to the Health Platform and the Shared Medical Card.

First, in connection with the changes to the Health Platform, the Capital Region should have identified relevant test scenarios in relation to updates and the connection between the Health Platform and the Shared Medical Card. These tests should have been completed before the changes were implemented as "all likely error scenarios are to be tested in connection with the development and modification of software if personal data are processed ", regardless of whether third parties make the changes or not.

Second, the Danish Data Protection Agency stated that the clarifying of responsibilities and roles was to be utilised in an agreement on governance mechanisms. According to the decisions, minimum measures in such an agreement are to "ensure that data controllers are in control" and to "prevent misunderstandings in data formats or service structure leading to loss or corruption of data integrity".

Third, and related to the required governance mechanisms, the Danish Data Protection Agency described a notification mechanism as one that needs to be established. This duty implies a proactive obligation to notify code changes to the data controllers of connected systems before the changes are activated (go into production). This duty aims to give the other controllers a realistic chance to conduct their own appropriate tests, and risk assessments. Furthermore, the notification mechanism contains a reactive element, as all stakeholders must be notified if errors are found when systems are integrated. This reactive notification should presumably ensure that the other controllers can investigate whether they have received compromised personal data and take action in order to correct the data, cf. also Article 5(1)(d) of the GDPR, according to which inaccurate personal data must be corrected or deleted immediately.

To summarise, according to the GDPR, public bodies are obliged to perform a risk assessment and implement appropriate measures to ensure data accuracy and integrity when establishing and performing data sharing. Further, they are obliged to clarify the GDPR's responsibilities and roles and draw up an agreement that ensures proactive and reactive measures in relation to changes and thereby mitigate the risk of processing incorrect and/or corrupted personal data.

5. *Future fruitful interaction between national administrative law and EU law*

There is no doubt that EU data-protection law is essential in order to prevent scandals such as the British post office-case, the Dutch SyRI-case or the Danish EFI-case or variations thereof. Article 5(1)(d) and (f) of the GDPR, combined with Articles 24-25 and 32, directs data controllers' focus towards proactive compliance procedures intending to ensure a sound organisation of data sharing and ensure continuous and effective data accuracy. This is combined with obligations to conduct ongoing monitoring and establish cooperation mechanisms between the involved organisations, including notification procedures. However, the impact of the GDPR is somewhat limited as the purpose of the regulation is to protect natural persons from any adverse consequences of processing incorrect personal data. As mentioned in Section 1, erroneous data may also benefit citizens in an illegitimate manner and thereby undermine the principle of equality as well as trust in the public sector.

Whether incorrect data are or are not defined as personal data or not, accuracy is still crucial from the administrative-law perspective. Ideally, an administrative body should always base its decisions and actions on validated information as the aim is to realise the intention of the legislator, who provided the legal basis for said decision or action. It does, in principle, not matter whether this is in favour of a citizen or not. Expanding the proactive and system-oriented approach via administrative law may, therefore, be of great importance in supplementing the rights-oriented regulation in the GDPR. The Danish principles of (digital) administrative law require proactive

compliance procedures in order to ensure the accuracy of data to be shared among public bodies and clarity of responsibilities among the involved organisations. These proactive procedures are combined with a duty to continuously monitor a chain of connected systems sharing data. By introducing these principles, Danish administrative law has, so to speak, re-established the balance of the past. This may contribute to preserving the presumption of data quality in the public sector and, thereby, the efficiency of the partially or fully automated administration.

At the same time, the approaches and required procedures of Danish (digital) administrative law and the GDPR have striking similarities. These similarities allow Danish public bodies to coordinate combined 360-degree risk assessments, identify the relevant measures, and implement them while at the same time establishing cooperation for continuous monitoring of data flows in digitized public administrations. Coordination of compliance procedures holds a promising potential for lowering the burdens on the public administration.