European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 1, pp. 255-282
ISSN 2724-5969 - ISBN 979-12-5994-243-2 - DOI 9791259942432 19

National Reports

EUROPEAN UNION

edited by
Andrea CIRCOLO, Ph.D. in EU Law, University of Naples Parthenope
Angelo CORRERA, Ph.D. in EU Law, University of Naples Parthenope

EU DIGITAL COVID CERTIFICATE

Regulation (EU) 2021/953 of the European Parliament and of the Council of 14th June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic

An EU Digital COVID Certificate is a digital proof that a person has either tick icon been vaccinated against COVID-19 tick icon received a negative test result or tick icon recovered from COVID-19.

On 14th June 2021, the European Union formally adopted the Regulation establishing a common framework for an EU COVID digital certificate covering vaccination, testing and recovery in the context of the COVID-19 (coronavirus) pandemic.

Since March 2020, EU Member States have taken several measures to limit the spread of the coronavirus and protect public health. Some of these measures have affected the right of EU citizens to move and reside freely within territories of Member States. During summer 2020, when incidence rates fell in Europe but vaccines were not even on the horizon, it was hoped that interoperable contact tracing apps would boost inter-European travel. This, for various reasons, did not happen: contact tracing gateway started working too scant, and apps download rate was too low in most countries for them to serve as an efficient means to fight pandemic.

In early 2021, when vaccination campaigns began in Europe, it quickly became clear that a number of European leaders wanted to issue vaccination cards to be used for both domestic and international purposes. In March 2021, the Commission announced its plan to introduce a card that could certify not only the vaccination status of holders, but also recent test results or recovery status.

In order to facilitate free movement and ensure that the restrictions on free movement currently in place during the COVID-19 pandemic can be lifted in a coordinated manner, the European Union has established an interoperable vaccination certificate. This vaccination certificate should serve to confirm that the holder has received a COVID-19 vaccine in a Member State and should contribute to the gradual removal of the restrictions on free movement. In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council and in line with the principle of data minimisation, in particular, COVID-19 certificates should contain only the personal data strictly necessary to facilitate the exercise of the right to free movement within the Union during the COVID-19 pandemic. The EU COVID digital certificate contains the necessary key information, such as name, date of birth, date of issue, relevant vaccine/test/recovery information and a unique identifier. These data remain on the certificate and are not stored or retained when a certificate is verified in another Member State. Certificates will therefore only include a limited set of necessary information. These cannot be stored by the countries visited. In order to verify that, only certificate validity and authenticity is checked by verifying who issued and signed it. All health data remain with the Member State that issued an EU Digital COVID certificate.

THE EUROPEAN APPROACH TO ARTIFICIAL INTELLIGENCE

Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM (2021) 206 final, 21st April 2021

The EU's approach to artificial intelligence centres on excellence and trust, aiming to boost research and industrial capacity and ensure fundamental rights.

As part of the European Strategy for Artificial Intelligence, the European Commission published on 21st April, the proposal for a regulation on the European approach to Artificial Intelli-

gence, which proposes the first european legal framework on AI. The proposal, which represents a further piece that will compose the technological-legal mosaic of the EU, assesses that risks within Artificial Intelligence assets, with aim of safeguarding values and fundamental rights of the EU and the security of users; to this end, it also envisages a new coordinated plan on Artificial Intelligence 2021 that will simultaneously strengthen the adoption of AI and investment and innovation in the sector throughout the EU.

In general, the proposed Regulation provides for harmonised transparency rules applicable to all AI systems, while specific provisions are made for AI systems classified as "high risk", for which a specific definition is introduced, to meet certain mandatory requirements relating to their trustworthiness.

The proposal for a regulation provides for the following prohibited AI practices, as they are contrary to EU principles and fundamental rights:

a) the placing on the market, putting into service or use of AI systems using subliminal techniques beyond a person's awareness in order to materially distort a person's behaviour in such a way as to cause or be likely to cause that person or another person physical or psychological harm;

b) the placing on market, putting into service or use of AI systems exploiting any vulnerability of a specific group of persons, due to their age or physical or mental disability, with the intention of materially distorting their behaviour in a way which causes or is likely to cause physical or psychological harm to them or to others;

c) the placing on market, putting into service or use of AI systems by or on behalf of public authorities which assess or rank the trustworthiness of natural persons over a specified period of time on the basis of their known or predicted social behaviour or personality traits or characteristics by means of a social score that determines either or both of the following:

- prejudicial or unfavourable treatment of certain natural persons or entire groups of natural persons in social contexts which bear no relation to the contexts in which the data were originally generated or collected;
- prejudicial or unfavourable treatment of certain natural persons or entire groups of natural persons which is disproportionate to the seriousness of their social behaviour;

d) the use of "real-time" remote biometric identification systems in publicly accessible areas for law enforcement purposes, unless and to the extent that such use is strictly necessary for one of the following reasons:

- the targeted search of potential victims of crime, including missing children;
- the prevention of specific and imminent threats to human life or terrorist attacks;
- the detection, tracing, identification or prosecution of an offender or suspect of an offence punishable by a maximum sentence or measure of at least three years.

However, a number of specific requirements are defined for using of such biometric identification systems

This innovative European approach also includes a proposal for a regulation on machinery, which lays down the safety requirements for products, replacing the current "Machinery Directive" no. 2006/42/EC.

It is recalled that this European approach follows a series of initiatives undertaken in recent years, including: the public consultation on the White Paper on Artificial Intelligence; the Final Ethical Guidelines for Trustworthy Artificial Intelligence, by the High Level Group on Artificial Intelligence, published on 8th April 2019; Report on Accountability for Artificial Intelligence and Other Emerging Technologies, by the Expert Group on Accountability and New Technologies, published on 21 November 2019; the Declaration of Cooperation on Artificial Intelligence, signed by 25 European countries on 10th April 2018, which builds on the achievements and investments of the European research and business community in AI and sets the basis for the Coordinated Plan on AI.

THE DIGITAL SERVICES ACT PACKAGE

Proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM (2020) 825 final, 15 December 2020

Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM (2020) 842 final, 15 December 2020

The Digital Services Act and Digital Markets Act encompass a single set of new rules applicable across the whole EU to create a safer and more open digital space.

The European Union is focusing its efforts on

creating a modern legal framework aimed at guaranteeing the security of online users, establishes governance that is consistent with the protection of fundamental rights and ensures that the activities of online platforms take place in a truly fair and open environment. In this context, on 15th December 2020, the Commission put forward two ambitious legislative proposals to update the rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA), which introduce horizontal rules intended to apply to all services and all types of illegal content, including goods or services, without replacing or amending, but complementing, existing specific legislation.

The DSA and the DMA, which are part of the broader strategy anticipated by the Commission in its Communication "Shaping Europe's Digital Future" and of the Union's "digital sovereignty" policies, hold two main objectives: to create a safer digital space where the fundamental rights of all users of digital services are protected; and to establish a level playing field to promote innovation, growth and competitiveness, both in the European single market and globally. European values are placed at the heart of both proposals and, in this sense, they complement the European Democracy Action Plan to make democracies more resilient.

In concrete terms, the DSA, making a work of rationalisation of the existing legislative framework, foresees a series of new harmonised obligations for digital services at the EU level, proportionate to the size of such services, through the introduction of new rules for the removal of illegal goods, services or content online; new safeguards for users whose content is mistakenly deleted from platforms; new rules for large platforms that will have to adopt risk-based measures to prevent possible abuse; measures to ensure greater transparency, including with regard to online advertising and the algorithms used for user profiling; new powers to verify the functioning of platforms, including by facilitating access to key data of these platforms; new rules on the traceability of commercial users in online marketplaces, to help identify sellers of illegal goods or services; and, finally, an innovative cooperation process between public authorities to ensure effective enforcement of the new rules across the single market.

In this context, platforms reaching more than 10% of the EU population (45 million users) are considered to be systemic in nature and are subject not only to more penetrating obligations to take down online content quickly, but also to the introduction of a new surveillance structure. This new accountability framework will include the work of national digital services regulators and the Commission, which will have specific powers to supervise large platforms, including the possibility to sanction them directly.

DMA deals, instead, with competition law profiles and, in particular, with negative consequences deriving from certain behaviours of platforms that have assumed the role of gatekeeper of the access to the digital market. In other words, these are platforms that have a significant impact on the internal market, that enjoy a particular position of relevance and that, for these reasons, can raise barriers to the entry of new companies on a given market. In concrete terms, the project of the Commission considers as such the enterprises which, on the basis of a quantitative criterion, invoice in a year at least 6.5 billion Euros in the EU or which have at least 45 million users among the citizens of the Union, as well as those which, on the basis of a qualitative criterion, even if of smaller dimensions, hold positions of particular importance on specific markets. In this perspective, the DMA will only apply to the main service providers of online platforms most prone to unfair practices, such as search engines, social networks or online intermediation services, which meet above-mentioned objective legislative criteria to qualify as gatekeepers. The proposed regulatory framework is based on techniques of preventive intervention, through the provision of rules that aim to prevent anti-competitive behaviour ex ante, rather than to sanction any violations ex post, and on a strict framework of sanctions, with fines of up to 10% of the worldwide turnover of the responsible company, with further aggravation in case of recidivism.

On the DSA and the DMA, which currently constitute the European response to the reflection process in which the Commission has been engaged over the last few years to understand the effects of digitalization - and more specifically of online platforms - on fundamental rights and competition, are now to be discussed by the European Parliament and the Council under the ordinary legislative procedure. If adopted, the final text will be directly applicable throughout the European Union.

GDPR: CONDITIONS FOR THE EXERCISE OF THE NATIONAL SUPERVISORY AUTHORITIES' POWERS WITH RESPECT TO THE CROSS-BORDER PROCESSING OF DATA

Court of Justice of the European Union (CJEU) (Grand Chamber), judgment of 15th June 2021, Case C-645/19, Facebook Ireland Limited and Others v Gegevensbeschermingsautoriteit - Request for a preliminary ruling under Article 267 TFEU from the hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), made by decision of 8 May 2019, received at the Court on 30 August 2019

Under certain conditions, a national supervisory authority may exercise its power to bring any alleged infringement of the GDPR before a court of a Member State, even though that authority is not the lead supervisory authority with regard to that processing.

On 11st September 2015, the President of the Belgian Privacy Commission (CPVP) brought an action for an injunction against Facebook before the *Nederlandstalige rechtbank van eerste aanleg Brussel* (Dutch-language Brussels Court of First Instance, Belgium) aimed at putting an end to breaches, allegedly committed by Facebook, of data protection laws. Those infringements consisted, inter alia, in the collection and use of information on the browsing behaviour of Belgian internet users, whether or not they have a Facebook account, by means of various technologies such as cookies, social plug-ins or pixels.

On 2 March 2018, Facebook appealed against that judgment before the Hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), the referring court in the present case. Before that court, the Belgian Data Protection Authority (DPA) had in the meantime legally succeeded the President of the CPVP.

The referring Court harboured doubts as to the impact of the application of the 'one-stop shop' mechanism provided for by the RGPD on the powers of the DPA and raised, more particularly, the question whether, in respect of facts subsequent to the entry into force of the GDPR (25th May 2018), the DPA could take action against Facebook Belgium, given that it is Facebook Ireland which has been identified as the controller of the data concerned. Indeed, as from that date and in particular in application of the 'one-stop shop' principle provided for by the GDPR, only the Irish Data Protection Commissioner would be competent to bring an action for an injunction, under the supervision of the Irish courts.

In its judgment, delivered in Grand Chamber, the CJEU specifies the powers of national supervisory authorities under the GDPR. In that regard, it states, in particular, that, subject to certain conditions, the Regulation authorises a supervisory authority of a Member State to exercise its power to bring an action before a court of that State and to take legal proceedings in the event of an alleged breach of the GDPR, with regard to a cross-border processing of data, even though it is not the supervisory authority in charge of that processing.

In particular, the Court specified, on the one hand, that the GDPR must confer on that supervisory authority the power to adopt a decision finding that such processing infringes the rules laid down in that Regulation and, on the other hand, that this power must be exercised in compliance with the cooperation and consistency procedures laid down in that Regulation.

EXTRACTION AND/OR RE-UTILISATION OF THE CONTENTS OF A DATABASE

Court of Justice of the European Union (CJEU) (Fifth Chamber), Judgment of 3 June 2021, Case C-762/19, CV-Online Latvia - Request for a preliminary ruling under Article 267 TFEU from the Rīgas apgabaltiesas Civillietu tiesas kolēģija (Regional Court, Riga, Civil Law Division, Latvia), made by decision of 14 October 2019, received at the Court on 17 October 2019

An internet search engine, which copies and indexes a database freely accessible on the internet and then allows its users to search that database on its own website according to criteria relevant to its content, is 'extracting' and 're-utilising' that content, which may be prohibited by the maker of such a database where those acts adversely affect its investment in the obtaining, verification or presentation of that content, namely that they constitute a risk to the possibility of redeeming that investment through the normal operation of the database in question.

CV-Online, a company under Latvian law, operates the website *www.cv.lv*, this site includes a database, developed and regularly updated by CV-Online, which contains job advertisements posted by employers. The www.cv.lv website also contains meta tags of the 'microdata' type. These meta tags contain, for each job vacancy contained in the database, the following keywords: 'name of post', 'name of undertaking', 'place of work' and 'date of publication of the vacancy'.

Melons, also a company incorporated under Latvian law, operates the website

www.kurdarbs.lv, which is a search engine specialising in job advertisements. That search engine makes possible to search various websites containing job advertisements according to various criteria, including the type of post and the place of work. By means of hyperlinks, the *www.kurdarbs.lv* site redirects users to the Internet sites where the information sought was first published, including the CV-Online site.

CV-Online, taking the view that there has been an infringement of its sui generis right under Article 7 of Directive 96/9, brought legal proceedings against Melons. It claims that Melons 'extracts' and 're-utilises' the substantial part of the contents of the database on *www.cv.lv*.

The court of first instance found that this right had been violated.

Melons appealed against the judgment to the Rīgas apgabaltiesas Civillietu tiesas kolēģija (Riga Regional Court, Civil Affairs Division, Latvia), which referred the matter to the Court, asking the following two questions: 1) 'Should the defendant's activities, which consist in using a hyperlink to redirect end users to the applicant's website, where they can consult a database of job advertisements, be interpreted as falling within the definition of 're-utilisation' in Article 7 (2)(b) of the Directive of 11st March 1996 on the legal protection of databases, more specifically, as the re-utilisation of the database by another form of transmission?' - 2) 'Should the information containing the meta tags that is shown in the defendant's search engine be interpreted as falling within the definition of 'extraction' in Article 7(2)(a) of the Directive of 11st March 1996 on the legal protection of databases, more specifically, as the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form?'

According to Court, concepts of 'extraction' and 're-utilization' must be interpreted as referring to any act consisting, respectively, in appropriating and making available to the public, without the consent of the maker of the database, the results of his investment, thereby depriving the latter of income which should enable it to amortise the cost of that investment.

It follows that such a transfer of the substantial contents of the databases concerned and such a making available of those databases to the public, without the consent of the person who created them, are, respectively, measures for the extraction and re-utilisation of those databases, prohibited by Article 7(1) of Directive 96/9, provided that they have the effect of depriving that person of income which should enable him to recover the cost of that investment.

Therefore, these must be considered as prohibited if the obtaining, verification or presentation of the contents of the database concerned demonstrates a significant investment and, secondly, if the extraction or re-utilisation in question constitutes a risk for the possibilities of amortisation of that investment.

LIMITS TO DATA ACCESS AND CRIMINAL LAW

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 2st March 2021, Case C-746/18, Criminal proceedings against Prokuratuur (H.K.) - Request for a preliminary ruling under Article 267 TFEU from the Riigikohus (Supreme Court, Estonia), made by decision of 12 November 2018, received at the Court on 29 November 2018

Access, for purposes in the criminal field, to a set of traffic or location data in respect of electronic communications, allowing precise conclusions to be drawn concerning a person's private life, is permitted only in order to combat serious crime or prevent serious threats to public security In addition, EU law precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to such data for the purpose of conducting a criminal investigation.

In Estonia, H.K. was condemned for a series of crimes by a court of first instance to a term of imprisonment of two years, (sentence upheld on appeal). The minutes on which the finding of the abovementioned crimes was based were drawn up, inter alia, on the basis of personal data generated in connection with the provision of electronic communications services. The Riigikohus (the Supreme Court of Estonia), before which H.K. brought an appeal in cassation, raised doubts as to the compatibility with EU law of the conditions under which the investigating authorities had access to the data in question.

Those doubts relate, first of all, to the question whether the length of the period for which the investigating bodies have had access to the data constitutes a criterion enabling the seriousness of interference which that access causes with the fundamental rights of the persons concerned to be assessed. In this manner, where that period is very short or the amount of data collected is very limited, the referring court asked

whether the objective of combating crime in general, and not only serious crime, is capable of justifying such interference. Secondly, the referring court expressed doubts as to whether the Estonian Public Prosecutor's Office could, in the light of the various tasks entrusted to it by the national legislation, be regarded as an 'independent' administrative authority within the meaning of Tele2 Sverige (Judgment of 21st December 2016, Joined Cases C-203/15 and C-698/15) capable of authorising the authority responsible for the investigation to have access to the data in question.

In its judgment, the Court holds that the Directive on privacy and electronic communications, read in the light of Charter of Fundamental Rights, precludes national laws which allow public authorities access to traffic data or location data, which are capable of providing information on communications made by a user of an electronic communications system or on the location of terminal equipment used by him and of allowing precise conclusions to be drawn about his privacy, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being limited to procedures whose purpose is to combat serious crime or to prevent serious threats to public security. According to the CJEU, the length of the period for which access to those data has been requested and the amount or nature of the data available for that period have no bearing on that. Furthermore, the Court considers that that same directive, read in the light of the CFREU, precludes national laws which make the public prosecutor competent to authorise access by a public authority to traffic data and location data for the purpose of conducting a criminal investigation.

BELGIUM

edited by
Florian JACQUES, Teaching assistant at University of Namur and researcher at NADI-CRIDS
Julie MONT, Teaching assistant at University of Namur, researcher at NADI-CRIDS and lawyer at Namur Bar
Pierre-Olivier PIELAET, Teaching assistant at University of Namur, researcher at NADI-CRIDS and lawyer at Walloon Brabant Bar
Elise DEGRAVE, Professor at University of Namur. Director of research at NADI-CRIDS

USES OF FEDERAL DATABASES

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 38/2021 of 23 March 2021

The BDPA ruled on a refusal to erase personal data published in the Belgian Official Gazette.

In this case, the applicant requested erasure of personal data published in the Belgian Official Gazette within the context of an undertaking decrease in capital. When complying with Article 69 and 73 of the Belgian code of companies, the applicant's notary accidentally requested publication of personal data such as the amount perceived by the claimant and its bank account. The competent public authority refused to erase the data. The BDPA considers that there is no legal ground for the publication of data in the Official Gazette. These data cannot be considered as necessary under a legal obligation of the defendant as they are not explicitly mentioned in Article 69 and 73 of the Belgian code of Companies and are not necessary for the transparency purpose which underlies these Articles. Similarly, processing of the data is not necessary for public interest of maintaining official documentation source for which the defendant was vested. In absence of legal ground, the BDPA also found a breach of the data minimisation principle. In order to refuse the erasure of the plaintiff's data, the defendant mentioned that, under Belgian law, only rectification of documents published in the State Gazette was allowed. The supervisory authority however considers that no explicit allowance to erase data is not sufficient to constitute a valid exception to the right to erasure under Article 17, (3) GDPR. Hence, refusal to erase the unlawfully processed data also breached storage limitation principle. Therefore, the BDPA orders to comply with the erasure request of the claimant and issues a reprimand.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 61/2020 of 8th September 2020

The BDPA received complaints from three persons following the consultation by a public authority (municipality) of the data contained in the National Register of the Claimants

The first claimant had deposited waste illegally on the territory of the municipality. The BDPA considers that, on the basis of the munic-

ipal regulations in force, the public authority could consult and process the data in the National Register of the first complainant who had deposited the waste, in order to send him an infringement report (processing necessary to carry out its task as a public authority). The data of the second claimant, the legal cohabitant of the first, were also consulted. However, according to the supervisory authority the processing of these data was not lawful as it was not necessary for the exercise of the public authority. Hence, his data could not be mentioned in the report. The same applies to the family relationship between the first and second claimants (cohabitants) and the second and third claimants (the third claimant being the father of the second claimant), which are irrelevant to the purpose of the municipality's decision. The Authority finds infringements of Articles 6(1)(e) and 5(1)(d) and (c) of the GDPR. Therefore, it issues a reprimand to the public authority.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 81/2020 of 23 December 2020

The BDPA condemned a parking company and a bailiff's office for – among others infringements of the GDPR - illegal consultation of the DIV register (vehicle registration database)

The Data Protection Authority sanctioned an undertaking specialized in street parking, which had accessed the data available at the DIV (vehicle registration database) the day after the complainant's vehicle had been checked. On that occasion, the undertaking processed the complainant's personal data (name, first name and address) without necessity. Indeed, at the time of the processing, the complainant still had the opportunity to pay the fee and the processing of these data (necessary for example to send a payment reminder) does not comply with the principle of data minimisation. Breaches of Articles 14, (1) and (2) of the GDPR (duty to inform), Article 15, (1) (right of access) and Articles 5, (2) and 24 (1) (obligation to put in place adequate technical and organizational measures to ensure the effective rights of data subjects and compliance with the principle of data minimisation) were established against the parking company. The company, as well as the bailiff's office in charge of the recovery (for other breaches to the GDPR) were reprimanded, fined, and forced to comply with the requirements of the GDPR.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 48/2021 of 8 April 2021

The BDPA ruled on the lawfulness of the search by a notary of the address of one of her former employees in the National Register database

In this case, the defendant was a notary who owed a number of "ecocheques" to one of her former employees (i.e. the plaintiff). In order to ensure that the Ecocheques were sent to correct address (due to the fact that the plaintiff had changed her residence but not her legal domicile during the contract), the defendant, in his capacity as a notary, consulted the National Register, a database to which access is strictly limited, in order to verify this.

The BDPA considered that the notary had not carried out any data processing that corresponded to the tasks within the scope of the competences for which access to the register data is granted to notaries. Therefore, this processing had no legal ground and therefore violated Article 6 in conjunction with Article 5.1.a) of GDPR.

Although the court noted that the notary's function did not plead in her favor, it nevertheless reprimanded the defendant, noting mitigating circumstances such as the fact that she had put in place measures and mechanisms to protect personal data and that the illegal processing was not structurally part of her office.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 54/2021 of 22st April 2021

Authority examined the lawfulness of the processing of household composition data by an association granting family allowances via the database of the National Register. This data also included the complete history of the composition of the household of the data subject and therefore personal data of third persons.

In this case, the applicant was the father of a person subject to family allowances. The father complained that when the association carried out a search to look at the composition of his son's household in order to grant him the correct amount of benefits due to him, it was at the same time taking note of the history of the composition of the household of the person concerned up to his birth. The father therefore considered that

the association did not have a valid reason to carry out this data processing.

In summary, the BDPA ruled that the processing of personal data of third parties not covered by the association's initial research was contrary to Articles 6, 5.1.c), 24 and 5.2 of the GDPR, since the data processing was not legal under the relevant normative texts and the association had failed in its duty to take measures to implement the principles of the GDPR.

In view of the issues at stake, the BDPA issued a reprimand to the association. It also drew the attention of the legal and technical actors involved to find together an appropriate technical solution for the applicant.

USE OF CITIZEN'S PERSONAL DATA FOR ELECTORAL PURPOSES

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 30/2020 of 8 June 2020

The BDPA received a complaint from a municipality whose officials had received election propaganda mail from a candidate for election.

In this dispute, decided by the Authority on 8th June 2020, a complaint was filed by a municipality against the defendant, the head of a political party list, for using a list of the municipality's staff (municipal employees) to send them election propaganda mail. The defendant, a candidate in the elections, used a list of municipal staff to send election mail. This involved 68 people, including the director general of the municipality and the data protection officer. This decision is interesting because it reminds us that legal persons, associations and institutions may, if they wish to denounce a breach of the GDPR, refer the matter to the Data Protection Authority, in the same way as natural persons. For the remainder, the Contentious Chamber considers that it is established that the personal data in the staff list were processed for other purposes than those for which they were initially collected (election propaganda). Thus, a breach of Articles 5.1.a), 5.1.b) and 6.1. of the GDPR is established vis-à-vis the defendant, who was the leader of the list in the elections. The defendant was fined EUR 5,000.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 39/2020 of 28 July 2020

On 28th July 2020, the Data Protection Authority dealt with a complaint from a resident of a municipality, who had received a postal electoral letter addressed to 'new residents' of the municipality.

The complainant argued that the party could only have known that she established herself in the municipality by using data other than the simple list of voters. After an investigation, the Authority's Litigation Division found that the party had compared the list of voters from 2012 with the list of voters from 2018 to determine who were the new inhabitants of the municipality. This is, according to the Authority, a violation of the purpose limitation principle. On the basis of the compatible purpose test, the necessity test and the balancing test, the supervisory authority finds that the processing is unlawful. The data controller has indeed modified and structured personal data to extract a "list of new inhabitants". In this respect, the litigation Chamber considers the unlawfulness to be sufficiently clear, given that the local electoral decree excludes the use and the consultation for comparison of the voters' lists for a purpose other than that those for which they were made available. The defendant (head of the party list) was reprimanded and fined EUR 3,000.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 53/2020 of 1st September 2020

In a decision of 1st September 2020, the BDPA once again examined the use by a mayor of a citizen's e-mail address, which had been obtained when the citizen in question had sent an e-mail to his secretariat a few years earlier to complain about a problem of public cleanliness.

In the opinion of the litigation Chamber, the citizen's e-mail address should have been processed only to answer a question. Therefore, it cannot be used to send him an electoral mail. The Chamber found several violations of the GDPR. First, a violation of the purpose limitation principle (Article 5.1.b.) and the lawfulness of processing (Article 6) as the defendant processed the complainant's data without a legal basis and in violation of the purpose for which the data were collected. Second, the Authority also considers that by sending the e-mail without checking the "blind copy" tool, the complainant's e-mail address was disclosed to third parties. Such disclosure does not comply with Article 33 of the GDPR (data leakage not notified to the

Authority). Finally, the respondent did not put in place technical measures to ensure that only the data necessary for each purpose were processed. The Authority imposed a fine of EUR 5 000 on the concerned mayor.

ELECTRONIC IDENTITY CARD

Cour Constitutionnelle de Belgique (Constitutional Court of Belgium), judgment 2/2021 of 14 January 2021

The Constitutional Court must rule on the constitutionality of Article 27 of the Belgian act of 25th November 2018 on the insertion of two fingerprints on the Belgian electronic identity card.

Following five actions against this provision, joined in a single case, the Court delivered its judgment on 14th January. In substance, the Court considers that although the taking of fingerprints constitutes an infringement of citizens' privacy, this interference is sufficiently regulated by law, necessary and proportionate to the aim pursued (which constitutes a ground of general interest within the meaning of Article 9 of the RGPD), namely the fight against identity fraud. The Court considers that the contested provision of the Belgian law merely implements, in advance, European Regulation 2019/1157, which aims to strengthen security and reduce the risk of identity fraud. Hence the Court considers that those objectives are legitimate and constitute objectives of general interest recognized by the EU law. The Court also ruled that the act clearly states that fingerprints will not be stored or centralized in any way, except during the period necessary for the production and issuance of the identity card (3 months maximum). With regard to the reading of the fingerprints on the card, the Court considers that it cannot be based on a registration of these data, which would prevent the cross-referencing of data for the purpose of identifying an individual. It also states that only border control staff, in Belgium and abroad, should be able to read this type of data, in the context of sufficiently specific tasks entrusted to them. The Court rejects the actions and confirms that the contested legal provision should not be annulled.

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 37/2021 of 16 March 2021

The BDPA received a complaint after the refusal of a municipality to deliver an identity card without the mention of the holder's title of nobility.

According to the defendant, the royal decrees of 8th January 2006 and 19th February 2019 require the mention of the nobility title in the National Register and the civil status documents. This information should therefore appear on the identity card for consistency purpose. The BDPA however notes that the title of nobility is not explicitly mentioned in the Act of 19th July 1991 (Article 6, §2) which lists the mandatory information of the Belgian ID card. In addition, principles of purpose limitation and minimisation imposes that only data necessary for the pursued purpose are processed. In the present case, the authority considers that a title of nobility is not necessary for the purpose of an identity document which must enable identification of a person. Even more, assessment of necessity must be reinforced when an ID document is used on daily basis. The BDPA finally recalls that technical and financial obstacles (i.e. modification of the IT system to withdraw nobility title of the ID card) cannot justify a refusal to withdraw an information of the ID card on request of the holder. The privacy by design principle requires continuous assessment of the technical aspects of data processing to ensure compliance with data protection principles. Therefore, a breach of Articles 5, 6 and 25 are established. In absence of possibility to fine the municipality, the BDPA issued a reprimand and ordered to establish a new identity card without the nobility title of the plaintiff.

DATA PROCESSING RELATED TO COVID 19 EPIDEMIC CRISIS`

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 24/2021 of 19 November 2021

In this decision, the BDPA ruled on the use of smart cameras by several coastal municipalities in order to measure, during the summer period, the influx of tourists at certain points of the dyke and in commercial areas.

We will focus on the points related to the lawfulness, necessity and proportionality of this measure, as well as on the analysis of the principles of privacy by design and privacy by default.

The Chamber found that the processing of personal data was based on the public interest task (6.1.e) of the controller, namely to protect the safety and health of the coastal inhabitants.

The Court ruled that this legal basis did not allow for a sufficiently precise determination of the processing of personal data, contrary to the requirements of Article 8 of the ECHR and Article 22 of the Belgian Constitution.

With regard to the proportionality and necessity of the measure, the chamber accepted the arguments of the defendant, noting that other manual counting tools did not achieve this objective, that the data were practically instantaneously anonymized and that the measure was limited both in space and time.

Finally, with regard to the principles of privacy by design and by default, the Chamber noted, in substance, that personal data were only stored locally on the cameras for a very short period of time before being anonymized. Therefore, these two principles were respected in this case.

COMPLIANCE OF THE PUBLIC SECTOR DATA PROCESSING WITH THE PRIVACY BY DESIGN AND PRIVACY BY DEFAULT REQUIREMENTS

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 83/2020 of 23th December 2020

The BDPA had to rule on the modalities to access to tax information documents stored on the Belgian tax administration (SPF Finances) website.

Until this decision citizens could use different means to access the website and two of them – which were the more convenient – were requiring authentication with personal or anonymous Microsoft accounts. In this decision, the BDPA founds that the SPF was the controller for the authentication procedure by means of Microsoft accounts. Authentication was closely linked to the purpose of using the defendant's website. Furthermore, the SPF determined the means of the processing by choosing to host its online services on Microsoft SharePoint. The BDPA found the practice as a breach of the loyalty and data minimisation principles combined with privacy by design/by default requirements for two reasons. First, Microsoft was processing personal data related to navigation activities on the website. In absence of dedicated information, processing of potentially sensitive data (possibly related to determination of the citizen's tax) was not loyal. This also applies because the BDPA found that, even if citizens may use anonymous accounts, the placing of cookies was impairing the capacity to remain anonymous. Second, as the citizen could use anonymous accounts (collecting less data), authentication by means of personal accounts was processing data unnecessary data for the purpose of accessing to the website. Additionally, the SPF did not pursue a DPIA despite the fact that Microsoft could link data related to the use of the website to the data it already detains about the concerned persons. Finally, the SPF was joint-controller for the placing of Microsoft's non-essential cookies through the website. Further browsing technique is not a valid consent vis-à-vis the use of these cookies. For these reasons, the BDPA issued a reprimand and ordered the publication of the decision on its website.

ADMINISTRATIVE FINES AS CORRECTIVE POWER AGAINST PUBLIC AUTHORITIES

Autorité de protection des données en Belgique (Belgian Data Protection Authority - BDPA) (litigation chamber), decision 73/2020 of 13th November 2020

The BDPA ruled on the possibility to issue fines against public undertaking vested with task of public interest.

In this dispute, the defendant is a social housing undertaking. The claimant filed six different complaints against the defendant for, among other use digital energy consumption meters transmitting personal data to a processor without any legal ground for the processing. It is recalled that the GDPR does not clarify nor define the notion of "public authority/body" under Article 83, (7) (optional exemption of administrative fines for public authorities). According to the BDPA, this provision and the Belgian Act of 30th July 2018 (Article 221, §3) which implement this possibility must be of strict interpretation. Hence, a social housing private undertaking can be fined for non-compliance with the GDPR rules event if it performs public interest tasks related to social housing. Consequently, and taking into account the financial situation of the defendant, the supervisory body orders the bringing into compliance of the processing operations and issue a fine of EUR 1,500.

In its decision 31/2020 of 16th June 2021, the litigation Chamber of the BDPA also ruled that an education authority of a school do not fall under the notion of "public authority/body" despite its tasks of public interest in the field of education.

Cour constitutionnelle de Belgique (Constitutional Court of Belgium), judgment 3/2021 of 14 January 2021

The Constitutional Court must rule on the constitutionality of Article 221, §2 of the Belgian Act of 30th July 2018 that exempts some public authorities from administrative fines in cases of breach of GDPR.

Under Article 221, §2 of the Belgian Act of 30th July 2018, administrative fines for breaches of GDPR cannot be imposed to public authorities which do not offer goods or services on the market. The claimant, an association for the representation of Belgian undertakings sought annulation of this provision. According to him, provision effects was discriminatory as it was exempting some data controller of the risk to be subject to fines. The Court recognises that both public authorities and private undertakings can act as data controller and process the same data. Thus, the provision creates a differentiated treatment. Nevertheless, the Court dismisses the claim for the following reasons: first, a possibility to fine public authorities vested with general interest missions may harm continuity of the public services by imposing additional financial burden to public authorities. Second, the legislator's choice does not exempt public authorities to comply with GDPR. In event of breaches of data protection rules, the BDPA may still use corrective measures against public authorities which can also be sentenced to criminal penalty. Furthermore, data subjects can still obtain compensation when public authorities are liable for a damage caused by GDPR infringements. Consequently, exemption of administrative fines for public authorities should be considered as proportionate because it protects public services - and ultimately citizens - from baring the weight of fines while leaving open the possibility to impose corrective measures.

FRANCE

edited by
Lucie CLUZEL-METAYER, Professor at the University of Paris Nanterre - CRDP, CERSA-CNRS

HEALTH DATA SECURITY

Conseil d'État (Council of State), ord. 13th octobre 2020, n°444937, Assoc. Le Conseil national du logiciel libre, dite Health Data Hub

The Higher Administrative Court of France considered that, even after the invalidation of the Privacy shield by the CJEU, of which Microsoft is a member, the risk of invasion of privacy is acceptable and so rejected the request for suspension of data processing. Nevertheless, the judge called on the public authorities by referring to the declaration of a change of host within two years by the Minister of Health.

The Health Data Hub (HDH) was created by law n°2019-774 of 24 July 2019 to centralise and facilitate the sharing of health data for the purpose of improving research, but also France's competitiveness in the AI race. Today, the HDH brings together 56 partners and manages the National Health Data System, which is set to become one of the largest health databases in the world. While the CNIL warned of the precautions to be taken when setting up this platform dedicated to particularly sensitive data, the decree of 21 April 2020 accelerated its implementation, in order to facilitate the use of the data in health crisis management. A contract was then concluded with a subsidiary of the American company Microsoft to host the data. When the case was first referred to the Conseil d'État, it initially considered that Microsoft, being a member of the Privacy Shield (Commission implementing decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the EU-US data protection shield), the choice to use its services did not present any risks (Council of State, ord. 19 June 2020, Health Data Hub Platform). But the invalidation of the Privacy shield by the CJEU (CJEU, 16 July 2020, C-311/18, B. Bertrand, J. Sirinelli, Dalloz IP/IT, Nov. 2020) changed the situation.

Once again, the Council of State, while maintaining a solution of rejection, notes this time the risks of transferring data to the United States for privacy. Although the order was issued within the limits inherent to emergency procedures, the judge made a more detailed assessment of the risks (B. Bertrand, Sem. Jur. Ed G. n°49, Nov. 2020, 1358; L. Cluzel-Métayer, AJDA n°13, April 2021, pp. 741-748). Initially, it considered that the contract protected health data: in reality hosted on the territory of the European Union, Microsoft had committed itself by way of an amendment to never process them outside the Union. After the invalidation of the Privacy Shield, a decree of 9 October 2020 took the precaution of prohibiting any transfer outside the EU. More delicate was the question of whether, outside the contractual framework, Microsoft, as a US company, could not be subject to potential transfer injunctions issued by the US intelligence services, due to the extraterritoriality of US law (section 102 of the FISA law and Executive Or-

der 12333). Although only marginally, Microsoft may have access to the data "in the context of unexpected or unforeseeable scenarios". The Council of State therefore found that the risk of having to respond to transfer orders was not zero. Nevertheless, it considered that the risk of invasion of privacy was acceptable and rejected the request for suspension of data processing for several reasons: firstly, because the risk is hypothetical since there is no direct violation of the RGPD, secondly, because all the data is anonymised and thirdly, because the public interest requires that the implementation of the HDH not be interrupted. The urgency thus justifies, in the eyes of the Council of State, maintaining the measure.

But if the judge does not suspend the implementation of the HDH, he nevertheless requires the parties to ensure that the system is brought into conformity. He enjoined them to conclude a new rider within fifteen days specifying that all services covered by the contract are indeed concerned by the transfer ban. In the spirit of compliance, it also makes various recommendations to the parties, including that of "seeking the best possible technical and organisational solutions to guarantee respect for the protection of personal data", in particular through regular audits. Also, and this is not the least of the original features of this decision, the judge calls on the public authorities to support his decision, by referring to the declaration of a change of host within two years by the Minister of Health. The Minister of Public Service and Transformation recently confirmed the migration of Microsoft's HDH data to a French or European cloud provider labelled "cloud de confiance" (A. de Montchalin, Stratégie nationale pour le cloud, Déclaration du 17 mai 2021). It will be interesting to look at this migration process, particularly from a contractual point of view, which will not only concern HDH data but probably all data held by French administrations.

OPEN DATA FOR COURT DECISIONS

Conseil d'État (Council of State), n°429956 du 21 janvier 2021, Ass. « Ouvre-Boîte »

The Council of State, while recognising the difficulty of making all court decisions available to the public, nevertheless enjoined the Minister of Justice to set a timetable for the open data of court decisions.

Provided for six years ago by the Law for a Digital Republic (Art. 20 and 21 of the Law of 7 Oct. 2016, amending Article L. 10 of the Code of Administrative Justice and inserting an Art. L. 111-13 in the Code of Judicial Organisation), the free online publication of all court decisions of the judicial and administrative orders is being implemented, not without difficulties (JCP G suppl. to n°9, 27th Feb. 2017). Taking up the recommendations of the Cadiet report (L'open data des décisions de justice, Nov. 2017), the 2018-2022 programming and reform law for the justice system was first to specify the conditions of this ambitious policy, by providing in particular for the concealment of the surnames and first names of natural persons, parties or third parties, and that of any element enabling the identification of the parties, third parties, but also judges and members of the court registry, when its disclosure is likely to undermine their security or the respect for the private life of these persons or their entourage. The possibility of re-using the identity data of judges and court staff to evaluate, analyse, compare or predict their actual or supposed professional practices was also prohibited (J.-B Thierry, JCP G n°19 13 May 2019). The aim was to prevent the rise of certain legaltech companies which, by putting justice into statistical perspective, aimed to predict the decisions rendered by judges. More than a year later, the implementing decree of 29 June 2020 still specified certain points, but left it to a decree to set the timetable for the implementation of open data for the judicial and administrative orders. When the decree did not come, the Court of Cassation (T. Perroud et al. Tribune, Dalloz Actu, 20 Oct. 2020 - Cass. 2e civ., 4 March 2021, No. 19-18.887 - Withdrawal), and then the Council of State were seized.

In its decision n° 429956 of 21 January 2021, the Council of State, while recognising the difficulty of making all court decisions available to the public, nevertheless enjoined the Minister of Justice to set a timetable for the entry into force of the provisions of the decree, as the "reasonable timeframe, more than 20 months after the law of 23rd March 2019 and more than six months after the publication of the decree of 29th June 2020", was, in the opinion of the high court, exceeded.

It was therefore under duress that the Minister of Justice adopted a decree, dated 28th April 2021, which provides for a staggered timetable until 2025 for the open data of court decisions. The regulatory authority could no longer escape its obligations.

GERMANY

edited by
Felix SCHUBERT, Ph.D. candidate in comparative public law, in cotutelle at the University Panthéon-Assas (Paris 2) and at Saarland University in Germany; research assistant at the Chair of French Public Law at Saarland University; "Volljurist"; "Diplomjurist"

NECESSARY INFORMATION ON THE POSSIBILITY TO FILE FOR LEGAL REMEDIES ELECTRONICALLY – THE SAGA CONTINUES

Pfälzisches Oberlandesgericht (Higher Administrative Court of Rhineland-Palatinate), judgement 8 C 11403/19 of 10 June 2020

The Higher Administrative Court of Rhineland-Palatinate had to rule on the question whether the wording "lodging an objection in writing or for recording" included the possibility to do so by means of an email.

In this case, a development plan (Bebauungsplan) was challenged before the Higher Administrative Court of Rhineland-Palatinate by the owner of a neighbouring plot. According to Section 10, paragraph 1 of the Federal Construction Code (Baugesetzbuch), development plans are under German law sub-statutory regulations (Satzungen), whose legality can be challenged before the administrative judge according to Section 47, paragraph 1, number 1 of the Administrative Court Procedure Act (*Verwaltungsgerichtsordnung*). The claimant invoked that the development plan was invalid due to a procedural irregularity. Drafts of development plans are to be published in order to give the public the opportunity to express concerns that can be taken into account before the resolution adopting the development plan is voted, pursuant to Section 3, paragraph 2 of the Federal Construction Code (Baugesetzbuch). The judges reminded that, in order to be valid, the publication needed to precise the modalities of how citizens could express their concerns. And that these modalities must not unduly limit the citizen's right to participate in the elaboration of development plans. In the case at hand, the possibility was given to lodge an objection "in writing or for recording (schriftlich oder zur Niederschrift)". The claimant invoked that this wording excluded the possibility to communicate by means of an email which restricted unduly the right to participate. The judges, however, ruled that the wording "in writing" is to be interpreted in a broad manner comprising also the possibility to use emails. And even if emails were not included, this should not constitute an obstacle preventing a citizen from participating in the development process; the citizen could require the administration to allow him to communicate by means of an email. The claim was dismissed.

Verwaltungsgericht Bayreuth (Administrative Court of Bayreuth), judgement B 4 K 18.821 of 30th September 2020

The Administrative Court of Bayreuth considered that an electronic document does not constitute any sub-form of a written document, but is a category of its own.

In another context, the Court of Bayreuth had to rule on a similar question: whether the information on the possibility of filing a suit "in writing or for recording" was to be understood to also include the possibility to use electronic means of communication. If yes, the information on legal remedies would have been sufficient, a limitation period would apply and legal actions that had not been taken on time would have been expired. If no, the information on legal remedies would have been incomplete, and the limitation period would not apply. According to the Court, the legislator created with the electronic document a whole new category of documents, that is not to be considered as a sub-form of the written document. Therefore, the wording "in writing or for recording" could not be interpreted to include electronic documents. Judges therefore did not dismiss the suit as expired.

Oberverwaltungsgericht Nordrhein-Westfalen (Higher Administrative Court of North Rhine-Westphalia), judgement 10 D 66/18.NE of 26th October 2020

The Higher Administrative Court of North Rhine-Westphalia differed expressly from the 10 June 2020 decision of the Higher Administrative Court of Rhineland-Palatinate.

Just like before Higher Administrative Court of Rhineland-Palatinate, the legality of a development plan was challenged before the Higher Administrative Court of North Rhine-Westphalia. And in the case at hand, the claimant also invoked (among others) that the wording "lodging an objection in writing or for record" was too restrictive and therefore limited unduly the citizen's right to participate in the planning process. This time however, the judges upheld the plea. They differed expressly from the High-

er Administrative Court of Rhineland-Palatinate's judgement. The North Rhine-Westphalian judges considered that the only relevant question was whether the wording could prevent certain interested citizens from participating. They found that yes, because a citizen could take the wording by the letter, and be demotivated by this apparent form requirement. Going further, the judges rejected the argument brought forward by their colleagues from Rhineland-Palatinate, that a citizen could, at least, require a participation by email, by considering that it could not be expected from a citizen to request interpretation aid from the administration concerning wordings which are unequivocally formulated. The judges annulled the development plan.

Verwaltungsgericht Kassel (Administrative Court of Kassel), court order 3 K 1008/18.KS of 5 March 2020 (Neue Zeitschrift für Verwaltungsrecht, 2020, p. 1133; H. Müller, Konkludente Eröffnung des elektronischen Rechtsverkehrs mit der Verwaltung durch Angaben im Briefkopf, in Neue Zeitschrift für Verwaltungsrecht, p. 1092; U.-D. Berlit, Rechtsprechung zu e-Justice und eGovernment 2019/2020 (Teil 1), in JurPC Web-Dok. 129/2020).

The Administrative Court of Kassel had to decide whether the indication of the administration's email address in an administrative act opened the possibility to lodge an objection electronically.

The claimant in this case was a student teacher in mathematics and chemistry aiming to pass her First State Exam. The First State Exam is in Germany a special end-of-study exam in some subjects, for example law, medicine or, in some states, for students aspiring to become teachers at school. In order to guarantee a uniformity and certain quality of the exam, is organised by the state, not the university, and it can be taken only a limited times before it is considered definitely failed. The claimant at hand failed her First State Exam in both subjects. She retook the exam in mathematics, but could not achieve the necessary result either. By decision of 10th May 2017, with reception on 12th May 2017, she was notified in writing that she had repeatedly not validated the First State Exam. The email-address of the administrative person responsible for this decision was indicated in the letterhead. The document contained the information that an objection against the decision could be lodged in writing or for recording within a month after reception. This one-month period results from the Federal Rules of the Administrative Courts (Verwaltungsgerichtsordnung (VwGO)), Section 70, paragraph 1. The claimant lodged an objection on 14th December 2017, more than seven months after reception, which was rejected by the administration as expired. The claimant then challenged this rejection before the Administrative Court of Kassel invoking that the information on legal remedies was incomplete, because it did not contain the possibility to lodge an objection electronically. The possibility to lodge this objection also electronically would have been required according to the claimant, because of the access for electronic documents opened in form of the email-address indicated in the letterhead. According to the Federal Rules of the Administrative Courts (*Verwaltungsgerichtsordnung* (VwGO)), Section 58, paragraph 2, a one-year period applies if information on legal remedies have not been given properly. Since the information was incomplete, according to the claimant, this one-year time-limit for the objection applied, instead of the one-month time-limit set forth in the decision, permitting her to still lodge the objection more than seven months after the reception of the decision. The judges ruled that the administration had not allowed for the electronic lodging of an objection neither explicitly, nor implicitly and that it was not obliged to do so, either. Even if an email-address was indicated, this did not implicitly open up an electronic access for documents requiring a qualified signature, like objections. The judges drew a comparison with a phone-number in the letterhead which would not open either the possibility to lodge an objection over the phone. The objection was therefore considered to be expired and the case was dismissed.

THE LEGAL EFFECTS OF ERRORS IN THE ELECTRONIC COMMUNICATION OF COURT DOCUMENTS

Bundesgerichtshof (Federal Supreme Court), judgement X ZR 119/18 (ECLI:DE:BGH:2020:140520UXZR119.18.0) of 14 May 2020

The Federal Supreme Court had to decide whether an appeal had been received in time and in the due form, although it could not be downloaded into the internal network of the court.

The appellant transmitted its appeal electronically through the "special electronic lawyer's

mailbox" (besonderes elektronisches Anwaltspostfach) on the last day of the deadline. It was subsequently saved on Court's receiving facility. However, for a reason that is not clear, the document could not be downloaded on the server which is used in the internal court network to access such documents. An error message appeared. The court suspected the problem to be a vowel mutation (ä, ö, ü) contained in the document's name. In order to confirm that the appeal had been lodged in time, the court analysed in a first step the requirements for the electronic reception of such an appeal. The relevant provision is the Civil Procedure Code, Section 130, paragraph 5, sentence 1. It provides that an electronic document is received as soon as it has been saved on the facility of the court that has been destined for the reception. Since the appeal had been well saved on the court's receiving facility on the last day of the deadline, it was considered received in time. In a second step, however, the court examined if a vowel mutation contained in a document's name could be considered as a mistake in transmitting the appeal. According to the Civil Procedure Code, Section 130, paragraph 2, sentence 1, the transmitted document must be suitable for a processing through the court. There is however no prohibition of vowel mutations for the electronic communication with the Federal Supreme Court. The judges found therefore that their presence in the document's name could not harm the lawfulness of the transmission/reception. It was therefore of no relevance, whether the document could then be treated internally or not as long as it had been correctly communicated and saved.

Niedersächsisches Oberverwaltungsgericht (Nordrhein-Westfalen Higher Administrative Court of Lower Saxony), court order 2 LA 686/19 of 15th May 2020

The Higher Administrative Court of Lower Saxony had to decide whether a violation of the court's duty to inform about errors in the electronic communication of pleadings justified an institutio in integrum.

The claimant in this case requested from the Higher Administrative Court of Lower Saxony the admission to appeal a judgement of the Administrative Court of Oldenburg of 16 September 2019 (case number: 2 A 7882/17) refusing asylum protection to the claimant. According to the Asylum Act Section 78, paragraph 4, sentences 1 and 4, a request for admission to appeal a decision has to be filed within one month as of notification of the decision. The judgement of the Administrative Court of Oldenburg has been notified on 19th September 2019. Within this deadline, on 8 October 2019, the claimant filed electronically a request for admission to appeal before the Higher Administrative Court. This request did however not present the necessary qualified electronic signature, in violation of Section 55a of the order on electronic legal transactions (*Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach*). In consequence of that, it was not valid. Another request has not been filed within the deadline. On 19 November 2019, the claimant filed for an *institutio in integrum* into the deadline, a fiction by which the claimant is considered to act still within a deadline that actually already has expired. Usually, in order to obtain such an *institutio in integrum*, the claimant has to demonstrate that he was, through no fault of his own, incapable to respect the deadline. The claimant could not provide any substantive arguments in that direction. The Higher Administrative Court granted nevertheless an *institutio in integrum*, because it considered that the court's procedural duty of care implies to inform the parties about procedural errors, like a missing qualified electronic signature, if there is still time to remedy these errors. Parties can legitimately expect the court to inform them in due time in order to prevent the expiration of procedural deadlines. While the duty of care is well established, this is an interesting application on electronic communication, especially an obligation of the court to verify the absence of errors in this special form of communication arises from it.

Oberlandesgericht Berlin (Appellate Court of Berlin), court order 5 W 1031/20 of 26th July 2020

The Appellate Court of Berlin had to decide how to deal with documents, that had been initially handed in electronically by the parties, then printed out by the subordinate Regional Court of Berlin in black and white, with no regard to possible coloured elements in these documents, and handed in in the context of an examination of the Regional Court's decision by the Appellate Court.

In this case, whose facts are of no further relevance, a claimant had a recourse to the Appellate Court of Berlin after the Regional Court of Berlin had rejected its demands for lack of jurisdiction. The Appellate Court of Berlin not only

annulled this decision. It also complained about the fact that the file handed in by the Regional Court of Berlin contained electronic party documents that were printed out by the Regional Court in black and white, without taking into consideration whether they initially had contained coloured elements. The Appellate Court considered that this fact alone would have been reason enough to refer the case back to the Regional Court, so as to give it the possibility to create an orderly paper file. The Appellate Court stated that it had no access to the initial electronic documents and could therefore not verify their conformity with the printed paper version. The judges also criticised that the Regional Court had repeatedly shown this procedure in the past. It reserved the possibility for the future to reject such files categorically, no matter if the only black-and-white colour was of any relevance in the individual case. They considered that it was simply not admissible for the Appellate Court judges to work with different documents than those handed in by the parties, and that it constituted a violation of the constitutional right to be heard provided for in the Fundamental Law, Section 103, paragraph 1 if the judges evaluated the handed in documents not in their authentic, but an altered form.

EXCEPTIONS TO OBLIGATIONS OF ELECTRONIC COMMUNICATION

Bundesfinanzhof (Federal Finance Court), judgement VII R 29/19 of 16 June 2020

The Federal Finance Court defined the not-inconsiderable effort allowing for an exception to the statutory obligation to transmit tax declarations electronically.

The claimant in hand was a self-employed physiotherapist, exercising without any employees, offices or consulting rooms. He had a PC as well as a telephone connection, but neither an internet connection, nor a smartphone. For 2017, he had declared an income of 14.534 € on a paper form, whereupon the tax administration required him to transmit the declaration electronically. Subsequently to his non-compliance, the tax administration imposed a penalty payment that was challenged by the claimant in court, before the Finance Court of Berlin Brandenburg. He won the case (Finance Court of Berlin-Brandenburg, judgement 4 K 4231/18 of 8th August 2019), but tax administration body appealed to Federal Finance Court. The obligation to transfer tax declarations electronically arises from the Federal Income Tax Act (Einkommenssteuergesetz), Section 25, paragraph 4, sentence 1. Pursuant to its sentence 2, the tax administration can exempt citizens from this obligation so as to avoid undue hardship. The exemption becomes mandatory for the tax administration according to the Federal Tax Code (Abgabenordnung), Article 150, paragraph 8, when the electronic transmission is unreasonable for economic or personal reasons. Pursuant to its sentence 2, alternative 1, unreasonableness is given especially when it would require a not-inconsiderable financial effort to establish the necessary technical connection and to procure the necessary equipment. This not-inconsiderable financial effort is however not further defined by the law. The Finance Court of Berlin-Brandenburg considered in its decision that this limit was exceeded when these efforts were in no economically reasonable relation to the income. The Federal Finance Court followed their colleagues from Berlin-Brandenburg and underlined that especially enterprises of the smallest size (Kleinstbetriebe) were to be targeted by the exception of the Federal Tax Code, Article 150, paragraph 8. The claimant was to be considered as such. Given the annual income of 14.535, costs for the soft -and hardware equipment, its maintenance, and the installation of an internet connection were judged to be considerable. Hence, the exception to the obligation of electronic transmission of tax declarations applied. And the tax administration's appeal was consequently dismissed.

Oberverwaltungsgericht München (Higher Administrative Court of Munich), court order 6 CE 20.2428 of 11 November 2020

The Higher Administrative Court of Munich had to decide whether an application for financial Covid-19-aid by the Bavarian state could also be handed in written form or exclusively electronically.

In this case, the claimant had applied for a financial Covid-19 aid provided by the Bavarian state under "guidelines for financial aid for self-employed artists affected by the Covid-19 crisis by the Bavarian Ministry for Science and Art of 27th May 2020" (Bayerisches Ministerialblatt Nr. 301.). According to number 6, sentence 4 of these guidelines, the application had to be made electronically. The claimant required the possibility to apply in writing, which was denied. Before the Administrative Court of Würzburg, he applied for legal aid to challenge the administration's refusal to accept his written application.

This request for legal aid was also dismissed (Finance Court Würzburg, court order W 8 E 20.1462 of 21st October 2020) which made the claimant apply before the Higher Administrative Court of Munich for legal aid to challenge the dismissal of his first legal aid request. To support his second application for legal aid, he invoked fears to disclose his personal financial data online, where they might "buzz around forever". He also referred to the Bavarian constitution, Article 3, paragraph 1, sentence 1 providing that Bavaria is a cultural state (*Kulturstaat*). Demanding an electronic application would turn this cultural state into a digital state, he alleged. These arguments could however not convince the judges. They did not exclude that a written application might have been admissible in exceptional cases, but reproached the claimant to not have substantially explained why an electronic application would have been impossible or unacceptable for him. His worries concerning the protection of his date were not sufficient. The constitutional argument was simply dismissed by the judges, and consequently as well the request for legal aid.

VIOLATION OF THE CONSTITUTIONAL REQUIREMENT OF SEPARATION FROM STATE AND PUBLIC MEDIA BY A TOWN'S WEBSITE

Landgericht München (District Court of Munich), judgement 33 O 16274/19 of 17th November 2020

The Federal Finance Court defined the not-inconsiderable effort allowing for an exception to the statutory obligation to transmit tax declarations electronically.

The claimants in this case were Munich newspaper publishers applying for an injunction against the private operator of the official website of the city of Munich. The website in question (www.muenchen.de, last accessed on 18 January 2021) represented itself to be the most visited Munich service website and one of the most successful city websites nationwide with 2.9 M visitors and 12 M page views. The website had an offer of 173,000 pages dedicated to a variety of topics ranging from "townhall" over "events", "cinema", "sightseeing", and "restaurants" to "shopping". The court did not follow the defendant's argument that the website was simply a permitted user-friendly marketing tool. It upheld the claimants' plea that the requirement of separation from state and public media was violated; a violation constituting an unlawful practise according to Federal Act against unfair competition (*Gesetz gegen den unlauteren Wettbewerb* (UWG)), Section 8 paragraph 1, Section 3 paragraph 1.

To this end, Court stated that the requirement of separation from state and public media resulting from the Fundamental Law, Article 5, paragraph 1, sentences 1 and 2 also applies to a private operator in charge of running a city's website. It authorises state media representation only within the limits of the public authority's competences and without detriment for the guarantee of free press resulting from the Fundamental Law, Article 5, paragraph 1, sentence 2. The claimants and the defendant were considered to be competitors, all competing for advertisement clients. Among many other examples, the judges found that articles covering the football club FC Bayern and the local store Konen or promoting a Metallica concert in the Olympia-stadium were presented in an editorial manner, comparable to daily newspapers. The content was not limited to the mere representation of facts and the layout so appealing that the limits of state media representation were exceeded. The judges issued an injunction order with a penalty payment of EUR 250.000 in case of non-compliance.

THE GDPR COMPLIANT USE OF WHATSAPP BY MUNICIPALITIES FOR THE COMMUNICATION WITH CITIZENS

Die saarländische Aufsichtsbehörde für Datenschutz (Saarland supervisory Authority for data protection), press release of 16 January 2020

The Saarland supervisory authority for data protection defined in a press release the conditions under which a communication of municipalities with citizens on WhatsApp would comply with the General Data Protection Regulation (GDPR).

The authority reacted to media coverage criticising the use of WhatsApp by certain Saarland municipalities. It analysed the municipalities' different offers to be contacted by citizens through WhatsApp, but could not find any violation of data protection rules. Although the authority questioned the GDPR-compliance of WhatsApp's metadata processing, it concluded that municipalities were however not to be considered responsible for this processing pursuant to Article 26 GDPR, because municipalities would not benefit from the processing which excluded joint controllership (Stefan Hessel, Is the

use of WhatsApp GDPR-compliant? Yes, says the Saarland Data Protection Authority in an investigation on the use of WhatsApp by municipalities, 16th January 2020, https://www.linkedin.com/pulse/use-whatsapp-gdpr-compliant-yes-says-saarland-data-authority-hessel/, last accessed on 18th January 2021). According to the supervisory authority, the municipalities would not transfer either any of the citizens' phone-numbers nor contact details to WhatsApp, for the app runs in a sandbox (Stefan Hessel, Is the use of WhatsApp GDPR-compliant? Yes, says the Saarland Data Protection Authority in an investigation on the use of WhatsApp by municipalities). It was up to the citizen himself to decide which information he reveals to WhatsApp. The content of the exchanged messages itself was also sufficiently secured by an end-to-end encryption, satisfying the authority's standards. Therefore, the supervisory authority permitted the municipalities' offer to be contacted by citizens through WhatsApp, but excluded that they contact citizens on this way without their prior consent.

ITALY

edited by

Antonio DI MARTINO, Ph.D. Student in Law Economics at University of Naples Federico II.

Pierantonio SAGARIA, Lawyer. Teaching Assistant in Admnistrative Law at LUM Giuseppe Degennaro University.

Sabrina TRANQUILLI, Ph.D., Postdoctoral research fellow in Admnistrative Law at University of Salerno.

DIGITAL APPLICATION IN TELEMATIC TENDERS

Consiglio di Stato (Council of State), sec. VI, decision 5008/2021 of 1st July 2021

Article 1, paragraph 2-bis, Law no. 241/1990, introduced the principle of fair cooperation principle between the administration and citizens; this one represents a clear expression of the constitutional principle set out in Article 97 of the Italian Constitution. The institute of "soccorso istruttorio" is applicable to candidates who find insuperable problems with the submission of an application to participate in a selection procedure, especially where the application is entirely digital. This rule also applies when the candidate has not demonstrated a brilliant knowledge to use digital methods, but the administration has not adopted appropriate tools to support the procedure and warn of the pitfalls of the application system.

The decision at issue analyzes the applicability of the "soccorso istruttorio" procedure in public tenders, in light of the very consolidated case law concerning the impossibility of applying this procedure when documents' omissions or procedural failures are required under penalty of exclusion by the lex specialis.

However, the State Council recalls that such reasoning cannot be applied in the following cases: a) the application for a selection was not submitted for reasons not imputable to the candidate's conduct; b) the non-submission of application is attributable to its basic technical incapacity, together with a lack of recovery tools and knowledge that could warn it about the technical dangers associated with submitting the application on the platform identified by the administration.

The case solved by the State Council concerns a platform for the submission and receipt of applications that is entirely digital and automated (SIRIO System); for this reason, if the administration does not declare the risks underlying the weaknesses and fragilities of the system - which in fact makes it particularly onerous the application to participate in the selection process - the "soccorso istruttorio" is possible, according with the principle of fair cooperation between the administration and citizens (specified in Article 1, paragraph 2, of Law no. 241 1990), even if the candidate has not adequately submitted the application to participate, and even before the starting of the procedure.

TRANSPARENCY IN TELEMATIC TENDERING SESSIONS

Consiglio di Stato (Council of State), sec. III, decision 627/2021 of 20th January 2021

The principle of publicity, as a direct corollary of the principle of transparency, constitutes an indefectible qualifying moment of the procedures of public evidence. However, tendering sessions carried out within a telematic platform do not have to be public, given the full traceability of the operations carried out, so there is no need for the publicity of the phase of bids opening and any potential damaging resulting from the breach must be proven in concrete.

The Italian Council of State dismissed the appeal of the runner-up in a tender procedure, which sought the invalidation of the entire procedure because the Commission had failed to inform competitors in advance of the day, time and place of the session for the opening of their bids.

The court reiterated that, in general, the principle of publicity, as a corollary of the principle of transparency, constitutes an indispensable qualifying moment of the public procedures also because of the relations of immediate and direct connection with the requirements of protection of competition and proper functioning of the market.

Hence the obligation to open the tenders in public session, in order to ensure that the integrity of the envelope and its contents is transparently ascertained at that time, so as to protect competitors from the risk of subsequent manipulation of the tenders, possibly due to the insertion, removal or alteration of documents.

The negative consequences are difficult to assess *ex post facto* once the seals have been broken and the packages opened, in the absence of an immediate finding, so it is considered that the protection must extend to cover not only the actual damage, but also the mere risk of damage to it, with the result that the breach of the obligation should necessarily lead to the re-opening of the tender.

Nevertheless, examining the case, the Council of State clarified that the principle of transparency must be combined with the principle of the potential offensiveness of the conduct, having specific regard to the regime of the individual selection procedure.

It is necessary to verify whether the violation of the rule of transparency is likely to affect, even potentially, but still in objectively appreciable terms, the proper development of the tender procedure.

In telematic procedures, this risk is remote, thanks to the full traceability of the operations and data flows between the individual participating operators, which guarantees an immediate and direct verification of the date on which the documents transmitted were packaged, their acquisition and any attempt to modify them.

The consequence of this reasoning is twofold.

Tender sessions carried out within a telematic platform do not necessarily have to be public. Anyway, it is for the party claiming infringement of the rule of publicity to demonstrate any potential damaging resulting from the breach, having regard to the specific telematic modalities of the tender.

LACK OF DIGITAL SIGNATURE OF THE PUBLIC PROCUREMENT ECONOMIC OFFER

T.A.R. Lazio, Roma (Regional Administrative Court of Lazio, Rome), sec. II, decision 12406/2020 of 23rd November 2020

The regional administrative court of Lazio ruled that the failure of the bidder to sign the economic offer constitutes grounds for exclusion and cannot be repaired. Not being able to check the computer used by participant (which had been disused after the application had been sent), the administrative judge called in a technical consultant to verify that the bid received by the central purchasing body was really unsigned.

The Italian national central purchasing Body (*CONSIP*) excluded a tender because of the lack of the digital signature by the legal representative of one of the bidding companies (part of a temporary grouping of companies).

The company challenged the exclusion before the administrative judge, even though the personal computer used to send the tender documents electronically had been yet decommissioned. Administrative Court appointed a technical consultant to ascertain whether the file received by *CONSIP* lacked the digital signature. The consultant carried out his investigation only on the documents produced by the applicant, without being able to verify the actual correspondence between those documents and those originally uploaded on the system.

Examination of *CONSIP* system log files shows that the tenderer uploaded a document without the signature of the legal representative of one of the companies and confirmed that it had been sent to the system. It should be noted that the warning messages produced by the electronic platform did not prevent the submission of files uploaded without a signature but had called the user's attention to the need to check the application.

Judges clarify that signing of an economic offer by all the members of a temporary grouping of companies is intended not only to identify the author of negotiating declaration, but above all to create, vis-à-vis the contracting authority, a collective obligation on the part of all the economic operators participating in the grouping. For this reason, the lack of a digital signature cannot be remedied after the expiry of the tender.

PORTUGAL

edited by
Luís PICA, Ph.D. candidate in Public Law, in The University of Minho (Portugal); Teaching assistant at the Polytechnic Institute of Beja (Portugal) and researcher

at JusGov-Research Centre for Justice and Governance
Sara SANTOS, Master's student at University of Minho; Associate Lawyer at Vieira de Almeida e Associados (Portugal)

EXERCISE OF THE RIGHT OF ACCESS TO ADMINISTRATIVE FILES

Tribunal Administrativo de Recurso - Norte (Administrative Court of Appeal - North), judgment of 21/05/2021

Within public administration, the right of access to nominative documents is assumed to be a request to administrative documents if said documents do not contain special categories of personal data.

Public administration is subject to the principle of open administration, foreseen in article 5 (1) of Law No. 26/2016 of 22nd August (LADA), which provides that "Everyone" has the right of access to administrative documents, including the right to consult and reproduce them, without any duty to provide reasons for such interest. However, the concept of "administrative document" includes only any content, or part of such content, which is in the possession of or held on behalf of the bodies and entities such as local authorities, whilst "nominative documents" are described as administrative document containing personal data, as defined in data protection regulations.

Notwithstanding the situations in which the access to nominative administrative documents may be restricted, the Court ruled that access to an administrative document with information on who and how much was received by elected representatives of a public entity could not be considered "personal data" under the legal provision referred to in paragraph b) of paragraph 1 of Article 3 of Law 26/2016 of 22 August. Although these data are intrinsically personal, they must be included within the concept of "administrative document".

In view of the provisions of Article 6, paragraph 9 of the LADA (as amended by Article 65 of Law No. 58/2019 of August 8th, which ensured the implementation in the internal legal order, of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, referred to abbreviated as the General Data Protection Regulation (GDPR)), the Court ruled that even if the documents requested by the Claimant's representative were deemed to be "nominative documents" the request would have still been considered to be based on the right of access to administrative documents, as documents did not contain any personal data which may reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

DIGITAL ASSINATURE AND PERSONAL DATA IN PUBLIC ADMINISTRATION

Tribunal Administrativo de Recurso - Sul (Administrative Court of Appeal - South), judgment of 08/04/2021

The court accepted that an insurance contract should be signed by the contracting rights through the digital signature, legitimizing the insurer to request information relating to the health of the insured provided that it proves legitimate interest in accessing information that under the legislation in force, is protected by understanding personal data of a sensitive nature.

Since the insurance contract does not present an autographed signature of the inheritance file, it is necessary to refuse that the document is not signed and, therefore, that it has not been concluded in compliance with the necessary formal conditions, since the signature can be made through the various signature modalities that the law determines, in particular through that admitted by the digital signature. Furthermore, Public Administrations do not have jurisdiction to call into question the validity of the insurance contract or terms in which it was granted between the parties, because it constitutes a third party in relation to that contract and could have no rights or interests that can be asserted thereof. The court eventually ruled that the Public Administration cannot refuse access to health data and information that is in the possession of a public entity, because it is in question nominative administrative documents, restricted access, applying the following normativity: (i) Article 268(2) of the Portuguese Republic Portuguese, (ii) Article 85 of the Administrative Procedure Code, (iii) Law Nº. 26/2016, 22/08 approving the scheme for access to administrative and environmental information and the re-use of administrative documents, transposing Directive

2003/4/EC of the European Parliament and the Council of 28th January and Directive 2003/98/EC of the European Parliament and the Council of 17 November (LADA), (iv) Law No 12/2005 , of 1/26, approving the regime for personal genetic information and health information and (see) Law Nº 58/2019 of 08/08, which ensures the implementation, in the national legal order, of Regulation (EU) 2016/679 of Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.

Thus, access to information and nominative documents, in particular where they include health data, produced or held by the bodies or entities referred to in Article 4 of Law Nº. 26/2016 of 22/08, is only allowed to a third party who is authorized by the holder or by whom he demonstrates to hold a direct interest, personal, legitimate and constitutionally protected in the information, pursuant to Article 1(3) of Law Nº. 26/2016 of 22/08, thus showing the Insurer a legitimate interest and coming from a contractual relationship, may access the information that proves necessary and appropriate to the intended purposes, and a third party may not refuse its transmission, nor claim a contractual defect that comes from the lack of material or formal requirements.

ELECTRONIC SIGNATURE IN TENDERING

Supremo Tribunal Administrativo (Administrative Supreme Court), judgment of 08/04/2021

An electronic file/document, in PDF format, even when containing several documents, is a document in itself, therefore signature of such file implies the signature of all the documents which integrate it.

The Supreme Administrative Court analyzed the conditions for a single digital file signed with an electronic signature and containing several documents to be valid within a tendering process.

The Court ruled that a file/document in PDF format, which may contain or include in its content several documents, is still an electronic document. When signing a digital document with a qualified digital signature, the individual is unequivocally assuming its authorship and accepting its content. Moreover, the digital signature is valid for the entire document, regardless of where it appears or is found visually, including, any segments or parts of its content, in the certainty that if pages are inserted/removed or comments are added to the document, such changes will be marked and easily identified fulfilling the purpose set out in nos.5 and 1 of article 54 of Law no. 96/2015 which is to avoid calling into question doubts regarding electronic files which are not digitally signed, namely questions of integrity.

Therefore, the Court found that an electronic file/document, in PDF format, even when containing several documents, is still a single document and the signature of such file implies the signature of all the documents which it integrates.

PUBLIC SELE AND EQUAL AND EQUITABLE FUNDAMENTALS OF IMPUGNATION

Tribunal Administrativo Central do Sul (Central Administrative Court of the South), judgment of 21/04/2021

The Central Administrative Court of the South ruled that in the procedural sale made by electronic auction, may not one of the entities unsuccessful in a set of different auctions and winner in another set of auctions, contest the criteria used only for those in which it was unsuccessful and not challenging the equal criteria adopted in the electronic auctions in which it was the winner.

Having been promoted the sale of a property through electronic auction, the court pointed out that it does not violate the principle of progressivity the possibility that the computer platform allows the proposals that are submitted to be superior to each of them, so that each tender is higher than the previous one.

The invitation containing the conditions under which the auction would take place, having no change of rules or inside information, does not legitimize the applicant's claim that the rules set out in Article 30(1) (b) of Law Nº 96/2015 have been infringed, of 17 August, nor of the provisions of points b) and c) of Article 141 of the CCP, even more so when the contracting authority used in both auctions the same rules and the same platform, so it is not perceived as only in relation to the 2nd auction the Applicant considers that these rules are violating competition, in accordance with Article 140(3) of the CCP (those which in the previous auction allowed to be classified in 1st place).

SPAIN

edited by
Javier MIRANZO DÍAZ, University Oberta of Catalunya
Alfonso SÁNCHEZ GARCÍA, University of Murcia

DIGITAL TOOLS RELATED TO COVID-19

Tribunal Supremo (Supreme Court), Contentious-Administrative Chamber, Third Division, case 635/2021, 6th May, appeal number 150/2020

About the compulsory use of an electronic system for choosing a work place in the Public Health Service in times of pandemic.

This case analyses the appeal lodged by participants in a selection procedure for a job vacancy, as trainee staff within the various Spanish public health services and in relation with different professional specialties (Medicine, Pharmacy, Nursing, Psychology, Chemistry, Biology). That selection is made on the basis of the marks obtained in a previous evaluation process, which determines the order of the applicants.

The appeal rejects the legality of article 2 of Order SND/411/2020 of 13th May of the Ministry of Health, which amends Order SCB/925/2019 of 30th August of the Ministry of Health.

The 2019 Order recognized the possibility of choosing their job destination through an on-site system. Its way to operate allowed to delay the final choice of each applicant until the time immediately preceding his or her turn. Furthermore, this system provided that, in the event that the applicant did not appear at that time, he/she could do so at a later date, but subject to the availability of places at that time. As an alternative to on-site selection system, the 2019 Order established a telematic selection system.

However, the 2020 Order makes the electronic selection system compulsory. With the new operating way, in case of lack of selection at the time assigned to each applicant, this will be considered equivalent to their resignation, without any possibility of subsequent selection. In addition, the new electronic system only allowed for a delay in the selection of the destination, up to a limit of twelve hours before the start of the award session at which each candidate must participate.

The Supreme Court allows the appeal and annulled article 2 of Order SND/411/2020, given the following points:

- Despite the fact that article 14.3 of Administrative Procedure Act (number 39/2015) allows regulations to establish the obligatory use of electronic means for "certain groups of individuals who, due to their economic or technical capacity, professional dedication or other reasons, are accredited as having access and availability" to such means, the Court considers that the special condition of the group affected by the Order has not been duly motivated and accredited by the Administration, and the burden of proof in this regard must fall on it.

- The regulations issued by the ministers, given the wording of article 62.1.a) of Act number 40/2015, have an internal organizational vocation within their respective departments. Therefore, the Ministerial Order does not constitute the appropriate instrument for the extension of the obligation to relate electronically with the Administration, as development of article 14.3 of Administrative Procedure Act (number 39/2015). The Government would be called upon to carry out this development through Royal Decree. In addition, the declaration of the State of Alarm does not deprive the Government of those competences in which it must act by Royal Decree.

- The "normative" product called to regulate a specific public selection process has not vocation of permanence, so it would not be the appropriate means for the development of the possibility foreseen in article 14.3 of Administrative Procedure Act (number 39/2015).

- Article 11 of Organic Act number 4/1981, of 1st June 1981, about states of alarm, emergency and siege, does not include, among its objective scope of application, the possibility of introducing new cases of compulsory use of electronic means by citizens in order to interact with Public Administration.

- Article 4.3 of Royal Decree 463/2020 of 14th March, about the state of alarm, do not include in its objective scope of application the delegation to the Minister of Health of the possibility of imposing to citizens the obligation to interact electronically with the Administration.

Against this majority criterion, a dissenting vote was pronounced, in which it is upheld that the regulations relating to the state of alarm based on the Covid-19 pandemic, would have justified the imposition of an electronic system of choice, as a sectorial manifestation of the limitation of the right to free movement and permanence in public places, inherent to the state of alarm.

Consejo de Transparencia y Buen Gobierno - CTBG (Transparency and Good Governance Council), decision 901/2020, 7th April 2021

Privacy and data protection impact assessment regarding Covid-19 tracking applications are to be disclosed.

Following a request submitted by a citizen before the Ministry for Economic Affairs regarding access to information related to privacy and data protection impact assessment, access was denied alleging forthcoming publication of an amendment of the document based on article 18.1.a) of the Spanish Good Governance and Transparency Act which states that, "Requests relating to information that is in the process of being developed or published in general shall be denied, with a reasoned decision". However, the CTBG clarifies that Regulation (EU) 2016/679, in its article 35.1, that the privacy and data protection impact assessment shall be finalised before the treatment.

It follows that, both at the time of filing the application and at the time of issuing the decision on which the present complaint relates, the Administration had to have in its possession the document containing the initial impact assessment, prior to the implementation of the application. Consequently, as the Ministry recognizes, in the case we are talking of an existing document, and it cannot in any way be considered to be "in the process of being developed".

Similarly, the by then undergoing amendment of the assessment implies that the document "pending publication" is the emended one (the 2.0 version), and not the impact assessment itself. Consequently, the CTBG concludes that denial of access to it is not justified.

Consejo de Transparencia y Buen Gobierno - CTBG (Transparency and Good Governance Council), decision 803/2020, 19th February 2021

Software information related to Covid-19 and epidemiological surveillance is protected under.

The Surveillance System in Spain (SiViEs) is the technological platform that integrates all these epidemiological surveillance processes in Spain.

In this case, the claimant requested SiViEs system software documentation, documentation of the structure of the SiViEs database, and detail of under which software SiViEs is created and with which database management software and system is managed. That is, the claimant request access to virtually all information regarding the technological functioning of the application.

Before this demand, the Ministry for Science and Innovation, in charge of the application, denied access to the information grounded on prejudice to the guarantee of confidentiality or secrecy required in decision-making processes (provided in article 14.1.k of the Spanish Good Governance and Transparency Act).

After a meticulous review of the case and the legal framework, the CTBG argues that disclosure of such information can indeed it can facilitate the ability to violate the application and the sensitive data that it contains and manages, and in short, it would make it easier to "attack" the application.

The CTBG assumes that, as the complainant points out, specially protected personal data contained in the database are not being requested - cholera, HIV AIDS, leprosy, hepatitis, others, recently, COVID19. But, even with these safeguards, it maintains that providing the information and technical documentation claimed would jeopardize the protection of these data. Furthermore, it states, in order to reinforce its argument – but which in our view could be considered some sort of an argumentative leap–, that the harm to public security and data protection is real and not merely hypothetical. Consequently, it confirms denial of access to information grounded on the exception of confidentiality or secrecy required in decision-making processes – a conclusion based in sufficiently general reasons to, in our view, interpret that it can be applicable to other similar health care applications.

Consejo de Transparencia y Buen Gobierno - CTBG) (Transparency and Good Governance Council), decision 743/2020, 3th February 2021

Regardless of whether the source code of Radar Covid19 has been already published, access to the technical offer of the service provided should be granted.

The Spanish Ministry for Economic Affairs celebrated a contract with the company INDRA for the design, development, pilot and evaluation of a system that allows the traceability of contacts in relation to the pandemic caused by COVID-19. This contract was awarded using the "emergency procedure" which essentially allows for a direct award mechanism. The final budget of the contract was 273,171.50 euros.

In the present proceedings it is common ground that the Administration has made public the following information, also accessible to the complainant, concerning the contract to which the complainant seeks access and which has been processed by the emergency procedure:

(a) The Processing Agreement and the Procurement Agreement.

b) The source code of the Radar Covid app on the Github platform, specifically in the https://github.com/RadarCOVID URL, which includes documentation and reports on the App.

Under these circumstances, the claimant requires access to the copy of the "supporting memory, specifications, contract and any other administrative documents relating to the Radar Covid application". The Ministry refused, arguing confidentially of the offer – economic and commercial interests, article 14.1.h. of the Spanish Good Governance and Transparency Act– and relying on the previously published information, based on the However, the CTBG concludes that: (1) the offer cannot be completely declared confidential; (2) that the publication of the source code and other relevant information does not preclude the disclosure of other information such as the offers; and (3) that the Ministry is compelled to provide that non-confidential information to the claimant, even if it is not available on-line and even if the documents are physically located in the companies buildings.

PUBLIC PROCUREMENT AND SOFTWARE LICENCES

Comisión Permanente de la Junta Consultiva de Contratación Administrativa - Catalonia (Standing Committee of the Advisory Board on Administrative Contracting for Catalonia), decision 1/2020, 28th July 2020

The legal status of software maintenance contracts.

In Spain, a software license agreement provided to the Public Administration is a standardized program (supply contract), while in a software development contract is considered a tailor-made program (service contract). However, the Spanish Public Procurement Act does not expressly provide for legal regime to be applicable to software maintenance. Such maintenance necessarily entails the completion by IT companies of a successive activities aimed at obtaining a result other than a work or supply, which fits perfectly into the definition and characteristics of a service.

Nevertheless, it is very common in practice for software maintenance to be offered by companies through a support guarantee and to do so as an additional service to the provision of a standardized computer license. For these cases, according to the administrative body, it will be necessary to carry out an interpretative exercise of the subject-matter of the contract in order to determine its legal classification, and consequently, not in all cases it will be necessarily classified as a supply or as a service. If these additional services do not involve complex actions and are necessary for the normal development of the programme, then it will be classified as a supply. Conversely, when the services involve complex actions that exceed the normal development of the programme provided, it should be classified as a mixed contract (supply + service).

Tribunal Superior de Justicia. Sala de lo Contencioso – Galicia (High Court of Justice. Contentious Chamber - Galicia), case 799/2020, 6th March, appeal number 4581/2017

The Administration can require bidders and contractors to have property over digital applications used to perform the contract.

The claimant contests paragraph n.9 of the procurement documents, which provides that the contracting undertaking must have developed the set of applications necessary for the full execution of the contract, and that the programs installed or developed during the development of the contract will be owned by the awarding company. The claimant argues that the relevant fact is that bidders have a license to use the program they will use, and not property over it –as this same Administration has proclaimed previous awards of the contract, without motivating the change of approach.

The Court argues that, first of all, the Administration is under no obligation to follow the same procurement documents as in previously awarded contract. It is not bound by previous contracts, and therefore no motivation is needed in the change of approach. Secondly, it clarifies that the requirement of having its own programme is not classed as part of the solvency of tenderers –which would make it contestable–, but it is rather a technical requirement, for it refers to the subjective characteristics of the informatic application and thus to how the contract will be executed. And consequently, it concludes that it is lawful and in line with EU and national law to require bidders and contractors to have

property over digital applications used to perform the contract.

Tribunal Superior de Justicia. Sala de lo Contencioso – Asturias (High Court of Justice. Contentious Chamber – Asturias), case 2595/2020, 17th November 2020, appeal number 176/2020

The Administration can hold the use of a software until replaced, even if the contract with the provider have finished.

The subject matter of the case deliberates over the use, by a local authority, of an integrated digital package for municipal management that includes both tax collection and management. This service was provided by the undertaking "AUXILIAR DE RECAUDACIÓN S.L.", but the Administration decided to "re-municipalize" –that is, to recover full public management– tax collection and management systems.

Clause 5.4 of the procurement documents provides that "in case of termination of the contract, the award company must guarantee to the City Council the use of the programs in order to ensure the continuity of the service by its own means until the final solution is adopted by the city. City Council will immediately have such programs for its exclusive use, committing not to assign their use to third parties." 22 months after termination of the contract, the company reclaims restoration of the application, arguing that the reasonable time to replace the system should have been at most of 3 months.

The City Council explains that the delay was due not only the complexities of the IT processes itself but also specific practical difficulties that raised in the particular process, which required recovering the Collection Service of the City Council with the delivery of bulky documentation in a matter subject to legal deadlines for the prescription of taxes.

The Court is embodied with the justification of the Administration, and reminds that clause 5.4 of the procurement documents did not set maximum time or payment for use of the software, and that therefore the only limit is the provisionally of the use, understood in a wide manner. In sum, the public interest behind the necessity of maintaining essential services which depend of software applications, provides public bodies with extensive discretion power and significant prerogatives to keep the provisional use of these applications until replaced.

DISTRIBUTION OF CONSTITUTIONAL COMPETENCES ON ELECTRONIC PLATFORMS

Tribunal Constitucional (Constitutional Court), case 68/2021, 18th March 2021

On the constitutionality of article 347 of the Spanish Public Procurement Act, related to electronic procurement.

Paragraphs 3 and 5 of paragraph 3 of this article 347 were appealed before the Constitutional Court by the Government of Aragon (appeal of unconstitutionality 4261/2018). The appeal argued, first, that Article 347.3 LCSP, by imposing on autonomous communities how to organize "information services similar to the Public Sector Procurement Platform", infringed the regional administrations self-organization power.

The Constitutional Court understood that "the objective of ensuring the principles of transparency and publicity of tender notices (these principles, in accordance with STC 237/2015, FJ 8, should inspire public procurement and administrative action) give this rule a materially basic character which in no way limits regional action, beyond providing that information for insertion into the State platform". In other words, that the organizational autonomy of sub-national Administrations finds certain limits, always subject to the proportionality test, which enable, as is the case, the imposition of certain requirements that are understood to be basic.

However, the Court does consider contrary to the Spanish Constitution the term "exclusive and exclusionary" in the fifth paragraph of the article, which contains the obligation for the local public sector to publish –at its choice– the information of its contractor profiles on the regional or state platform: "local authorities, as well as those of their related or dependent entities may choose [...]". This paragraph prevents the sub-national authorities from imposing local authorities' publication on the regional platform, against which the Government of Aragon maintained that this election should correspond to the autonomous community, and not to the local entity.

The Court, as we say, sustains that "the basic thing in this case is the requirement of the publication by local authorities of their profiles on a procurement platform" and that "this requirement is satisfied with the publication in either, the state or the regional, or both". It therefore opens up a new possibility, which is the publication of the tender notices and other information required simultaneously on both platforms (state and autonomic), regardless of the relationship

between the latter. Therefore, against the argument of the what the Government of Aragon claimed, which understood that this choice on where the local public sector should be published was a matter for the autonomous community, the Court concludes that "the recipients of the provision are no other than the contracting bodies of the local authorities and it is for them to make the option unconditionally". In other words, Court seems to make it clear that the choice of platform on which to host this information was up to local entities, since in both cases –publication in national or regional platforms, or both– the ultimate objectives of transparency and efficiency were met.

DATA PROTECTION

Agencia Española de Protección de Datos – AEPD (Spanish Data Protection Agency), decision E/10900/2019, 10th September 2020

Collecting personal and biometric data of civil servants for work purposes.

In this case, the claimant held that for a long time, the system of presence control and the way of collecting personal and biometric data in the Teulada City Council do not guarantee the rights of workers and possibly violates the Data Protection Act. He argues that there is no HR certificating that the data is being encrypted and stored on the system.

The AEPD reminds some of the requirements set out by EU and Spanish law for data treatment. Firstly, it concludes that this kind of data treatment is considered personal data as defined in law, for it collects biometric information. Therefore, it requires a legal basis in order to be implemented. In this case, the AEPD considers that the situation meets the requirements of article 6 of the European Regulation, concerning the lawfulness of the processing, which in paragraph 1 (b) states that treatments shall be lawful if (b) [the] processing is necessary for the performance of a contract to which the person concerned is a party or for the application at his request for precontractual measures (...)".

In the present case, therefore, the biometric treatment for the control of presence in the workplace was considered to be in line with the GDPR as the City Council had established both the Registry of Processing Activities regulated in Article 30 of the GDPR and carried out the mandatory Impact Assessment relating to data protection regulated in Article 35 of the GDPR.

ERROR HANDLING IN PUBLIC EMPLOYMENT PROCEDURES

Tribunal Superior de Justicia. Sala de lo Contencioso – Murcia (High Court of Justice. Chamber for Contentious Matters - Murcia), case 122/2020, 6th March 2020, appeal number 4/2020

Error handling cannot be accepted if it contradicts the information recorded in the application.

In a competitive procedure for recruitment of public employees in the University of Murcia participated, among others, two women: Ms. Luisa and Ms. Rita. The latter appeared as excluded in the definitive list of admitted candidates because "the application was not submitted in a timely and correctly" according to the system. Ms. Rita lodged administrative appeal, which was estimated by resolution of 21 September 2017. Finally, a final decision was issued, assigning Ms. Rita the post of Team Leader (n.1), and Ms. Luisa the position (n.2) Assistant Service.

Ms. Luisa appealed before Court alleging that Ms. Rita only filled out the instance, but that it lacked the necessary electronic signature and therefore the application was not fully submitted. According to the claimant, the University could in no way admit the error handling as it did, for it is not a remediable defect.

The information registered in the application confirmed that the defendant had been using the platform and had registered some information within the deadline for submission. However, the signature process, which is according to the call for applications inherent to the submission itself, was never completed. Even though it is proved that the defendant tried to deliver the submission to completion and used the platform –as she tried to demonstrate by different means on trial–, the Court gives full credibility to the application informatic system, and the registries recorded. Therefore, it considers as proved the fact that the defendant did not complete the submission process, and that consequently there was no error to be handled, as there was no lawful application to be repaired.

The case demonstrates that someone who did not file the application cannot be admitted in proceedings (no rectification can be accepted). And at the time of assessing the proofs, the computer application prevails. Possible errors of the computer applications are not easily demonstrable, and the error is necessary requirement to allocate it to the functioning to the Administration.

ELECTRONIC ADMINISTRATIVE FILE

Tribunal Supremo (Supreme Court), Contentious-Administrative Chamber, Third Division, case 680/2021, 13th May, appeal number 5011/2019

About the requirements of the electronic administrative file.

In this case, the Supreme Court annulled the sanction imposed by the City Council of Las Palmas de Gran Canarias on the holder of a taxi license, consisting of the withdrawal of the license. The main reason for the annulment was that the sanction imposed by the City Council was based, essentially, on a report by the Spanish Tax Administration Agency, which showed that the license had been improperly exploited by third parties.

The use of the aforementioned report as sufficient evidence against the private, would have been contrary to the provisions of art. 95.1 of the General Tax Act, which declares the confidential nature of the data, reports or background information obtained by the Tax Administration in the performance of its competences. These may only be transferred to other administrations for purposes related with their own tax competences. To other purposes would be necessary the previous consent of the private. These requirements that would not have been observed in the present case.

However, beyond aforementioned main issues, it is worth highlighting the fourth legal ground, where are analyzed functional requirements of electronic administrative record provided by article 70 of Administrative Procedure Act (number 39/2015). Both the aforementioned article and article 48 of the Contentious-Administrative Jurisdiction Act require the administrative file to have an index that guarantees its integrity and immutability, as well as allowing an orderly consultation of all the documentation on file.

On the basis of the above, the court concludes that these requirements are not fulfilled with a simple scanning of the paper sheets of the administrative file, which would impede a quick search for the information of interest, "Causing the user to view each and every one of the sheets on the computer screen every time a document is consulted". Consequently, these files digitized in such way could not be considered as electronic files in the light of rules in force.

SUBSTANTIVE TIME LIMITS AND USING ELECTRONIC MEANS

Audiencia Provincial de Zaragoza (Civil Court of the Province of Zaragoza), Section number 4, case 287/2020, 20th November, appeal number 285/2020

Substantive time limits under the use of electronic means available every hour every day of the year.

This case analyses the computation of time limits in a court of law. However, it is of interest, given the possible parallels between article 135 of the Civil Procedure Act and articles 30, 31, 43 of Administrative Procedure Act (number 39/2015), 38 of Administrative Organization and Function Act (number 40/2015) and 41 to 44 of Royal Decree 203/2021.

In this judgment, the court recalls the distinction made by the Supreme Court between procedural and substantive deadlines. In line with the above, it points out that the only reason why the rule of procedural deadlines was applied to substantive deadlines, is due to the fact that if the last day of the deadline ended on a non-working day, because of the organization of the Administration of Justice, would be impossible to use its on-site register in order to bring their action. Consequently, as far as the integrity of the time limit must be respected, it was necessary to move its last day until to the next working day.

However, the Court has determined that this criterion needs to be changed in view of the possibilities offered by new technologies. Electronic systems deputies to information exchange and submission of documents, irrespective of the procedural effectiveness indicated, allow their use at all hours and on all days of the year. As a result, it is no longer necessary to apply the regulation of procedural deadlines to substantive deadlines. For this reason, if the end of the latter occurs on a non-working day, it will not be extended to the next working day.

In view of the above, the question arises as to whether this doctrine would be applicable, among other substantive time limits as administrative offences and sanctions expiration periods or as administrative limitation periods for claims related to patrimonial responsibility of the Administration, with respect to those privates obliged to interact electronically with the Administration, given the availability and operation of the electronic registration and notification systems every day and hour of the year.

USE OF ELECTRONIC MEANS IN TAX ADMINISTRATION

Tribunal Económico-Administrativo Central (Central Tax Administrative Court), decision of 22th January 2021, appeal number 4868/2020

About privates forced to interact electronically with Tax Public Administration in accordance with article 14.2 of Administrative Procedure Act (number 39/2015) and the obligation to notify previously through non electronic means about their inclusions in notification electronic systems.

As is established in the second legal ground of the Decision, the main issue analyzed "consists of determining whether, since the entry into force of Act 39/2015, of 1st October, about the Common Administrative Procedure of the Public Administrations (LPAC), it is necessary, for making electronic notifications to legal entities, a previous non electronic notification of the State Tax Administration Agency (AEAT) about their inclusion in the authorized electronic address system (NEO), as is provided by article 5.1 of Royal Decree 1363/2010, of 29th October".

In this endeavour, the Administrative Court points out that Administrative Procedure Act (number 39/2015) repeals Act 11/2007. It is pointed, besides, that Royal Decree 1363/2010 was adopted as development of the latter.

Such repeal must also entail a tacit repeal of the regulatory rules previous to Act number 39/2015, insofar as they contradict the latter.

In this regard, a distinction is made, firstly, in the case of taxpayers who must use electronic means by application of article 4.2 of Royal Decree 1363/2010 and who are not covered by article 14.2 of Act number 39/2015. In these cases we can find a regulatory specification of article 14.3 of the aforementioned Law. Hence, the obligation to compulsorily interact with the Administration electronically allows its modulation in regulations and, therefore, the need to communicate on paper to taxpayers their inclusion in the electronic notification system.

However, with regard to taxpayers expressly designated by article 14.2 of Act number 39/2015, which are the legal entities and entities without legal personality referred to in art. 4.1 of Royal Decree 1363/2010, as well as those others that fall under the provisions of art. 4.2 of the aforementioned decree, "the obligation to notify their inclusion in the authorized electronic address system regulated in article 5.1 of the aforementioned Royal Decree must be understood as repealed, given that, in accordance with article 14.2 of the Administrative Procedure Act, they are forced, in all cases, to relate through electronic means with the Tax Administration".

The Administrative Court understand the unconditional obligation to interact electronically with the Administration of the subjects of art. 14.2 of Act number 39/2015, as a mandate that must repeal the previous conditions provided by regulations. That implies the application of the principle of hierarchy of norms, instead of the application of the principle of specialty.