Digital Autonomy in Contractual Relationships

Martin Nettesheim 2022-10-18T12:52:51

I. Disagreement between two Advocates General

It is rare for two Advocates General of the European Court of Justice to differ on the interpretation of a fundamental legal act of the European Union (EU). This is what recently occurred with regard to the General Data Protection Regulation (GDPR).

In his Opinion of 20 September 2022 (Case C-252/21, Meta Platforms, Inc. and Others v. Bundeskartellamt), Advocate General *Rantos* interprets the legal bases provision of Article 6(1) GDPR in the sense that the bases of lit. b) and lit. f) should be given as narrow a scope as possible in order to provide the widest possible scope of application to the basis of consent under lit. a) (paras. 53-65). His understanding of Article 6(1) GDPR aims to strengthen the possibility for data subjects to control "their" data, which is linked to the concept of consent under lit. a), which must be freely granted, and which can be withdrawn at any time. His objective is thus to facilitate arbitrary freedom of decision to the data subjects affected by data processing. The objective of free movement of data addressed in Article 1(1) GDPR plays no role in his considerations; that provision is not mentioned. The more general objective of the EU to establish functioning data markets in order to strengthen European competitiveness and to ensure a high level of prosperity of the European population does not have any importance for him either.

Advocate General *Campos Sánches-Bordona* takes an opposite point of view in his Opinion of 6 October 2022 (Case C-300/21, UI v Österreichische Post AG). He concedes that the data subject's consent should be seen "as the ultimate expression of control" (para. 73). However, he then goes on to state: "In my view, it is not straightforward to conclude from the GDPR that its objective is to grant data subjects control over their personal data as a right in itself, or that data subjects must have the *greatest control possible* over those data." (para. 74). In his view, it is not clear that control over data is part of the essential subject matter of the fundamental right under Article 8 Charter of Fundamental Rights of the European Union ("Charter"). During the legislative process of the GDPR, there was a suggestion to include a recital addressing the right of data subjects to "exercise control over personal data which is being processed"; however this proposal was not implemented. The extent to which the two Advocates General's Opinions differ from one another becomes evident when Advocate General *Campos Sánches-Bordona* explicitly mentions the GDPR objective to promote the free movement of data (para. 78) and then states that "[s]trengthening individuals' control over their personal information in the digital environment is one of the recognised aims of the modernisation of the rules on the protection of personal data, albeit not an independent or isolated aim." (para. 79). Rather, the objective should be read in context with the objective to enable "the

potential of the digital economy to be fulfilled and encourage[…] 'economic growth and the competitiveness of EU industries'" (para. 80).

The contrast between the two Opinions clearly reveals different philosophies on data protection. Identifying such divergences is not only of academic interest. The way one positions oneself has a direct impact on the interpretation of both Article 8(1) Charter and Article 6(1) GDPR. The discussion on how to understand data protection in the modern digital society has so far not clearly progressed beyond positions that were developed in times of predominantly state data processing in the bygone 20th century.

Below, this article will show that Advocate General *Campos Sánches-Bordona*'s understanding of data protection autonomy is clearly preferable to Advocate General *Rantos*'s approach (II.). This leads to conclusions concerning the relationship between data protection law and private autonomy (III.) as well as the interpretation of Article 6(1) GDPR (IV.). The article concludes by highlighting the importance of safeguarding the EU's digital competitiveness (V.).

II. Digital autonomy as arbitrariness or as design

With the adoption of the GDPR, the EU laid the foundations for establishing and preserving the level of digital protection guaranteed by Article 8(1) of the Charter. The challenge is to interpret the provisions of the GDPR – which, in many respects, are open and in need of concretization – in such a way that the goal of digital autonomy is actually fulfilled in the real world. In this context, a question of great significance is what space is granted to contracts whose subject matter is the provision of digital services. Questions of data protection law arise when these services are based on using personal information of the contractual partner. How should such contractual relationships be approached? Two basic views or protection philosophies appear to battle it out.

Digital autonomy as arbitrary "control"

At the root of the first, certainly older, protection philosophy is the position that digital autonomy essentially consists in having the possibility of permanent control over one's "own" personal data. Digital autonomy, at its core, is established by requiring people to provide their consent to any form of processing of "their" data and affording them the ability to withdraw their consent at any time. This data protection philosophy was developed in the 1970s for the relationship between the state and the citizen. It is now being extended to the circumstances of the digital society. According to this concept, control means retaining the decision as to whether one digitally appears at all as a person in the economy, culture and society, and furthermore, with which personal information this occurs. Important here is that this philosophy is now also to be applied in contractual relationships in the digital economy. This is regularly associated with the regulatory ideal that the dissemination of personal data should be minimized. According to this view, the aim must be to extend the scope of application of Article 6(1)(a) GDPR (consent under data protection law) as far as possible to contractual relationships as well. At the

same time, this means that the scope of application of other legal bases, especially Article 6(1)(b) GDPR, must be interpreted restrictively.

Digital autonomy as a right to shape social relations

On the opposite side, there is a protection philosophy that does not see the ideal of digital autonomy primarily in the power to control digital personal information in public spaces. According to this concept, digital autonomy means first and foremost being able to exert a formative influence on the use of personal information by third parties. Whoever wants to strengthen digital autonomy will, according to this view, work primarily towards making people's legal power more effective in enabling them to have a say in how their personal information is used in their economic and social relationships. How far this must go depends on the context. For the *area of digital-content contracts* that is of interest here, what matters most is that people (as contracting parties and data subjects) are empowered to enter into a fair and appropriate contractual commitment and to determine how their data is used in that context. Digital autonomy, according to this position, *also* includes the freedom to dispose of personal data as a good with market value. Autonomy cannot be reduced to the (misleadingly so-called) personal rights dimension of digital identity, but also extends to an economic dimension. Whoever wants to deny people digital autonomy in the market does not, according to this view, strengthen self-determination, but curtails it paternalistically.

The latter protection philosophy focuses on the right of people to enter (or refrain from entering) into contractual legal relationships that (also) regulate the use of personal information for mutual benefit. According to this view, digital autonomy also includes the freedom to dispose of personal data as an economic good with market value. It is not a loss but a gain of autonomy when a data subject grants a third party the contractual right to use personal information the processing of which is necessary to obtain a desired service (subject to reasonable restrictions, e.g., on data security, purpose limitation, appropriate retention periods and their other rights, including under the GDPR). Here, self-determination means recognizing that there is value in acquiring a service that requires the processing of data. Respecting the private autonomy of the data subject under data protection law protects self-determination; whoever relies on an arbitrary right of consent instead calls private autonomy into question.

Therefore, the expression of the use of true digital autonomy is not the isolating (and fragmenting) refusal of consent regarding the use of personal data, but the always socially integrating private autonomous agreement with third parties on whether and how the available personal information can be used. Naturally, this also includes the freedom not to enter into agreements in this regard and thus to prevent its use. However, this is then only one of many options – and not the guiding goal of the idea of digital autonomy.

According to the latter view, Article 6(1)(b) and Article 6(1)(a) GDPR are equal in normative terms. Where an effective agreement on the use of data has been reached, autonomy has manifested itself; there is no reason to add a requirement for consent at the level of service provision. Data contract law (including digital

consumer protection law) is of central and primary importance in enabling the level of protection envisaged in Article 8(1) Charter. The consent requirement of Article 6(1)(a) GDPR especially plays a role where there is a lack of contractual agreements expressing the autonomy of the data subject, i.e. above all in the case of access to personal data by third parties who lack a contractual relationship with the data subject.

The necessity of confronting one's own pre-understanding

Legal texts regularly do not govern the universe of meaning and the prior understandings that guide their interpretation and application. This also applies to the GDPR. Both of the above contrasted concepts of digital autonomy can form the basis for the interpretation and application of the GDPR. However, the decision for one of the concepts (or for intermediate constructs) regularly determines the interpretative outcome. In any case, when proposing an interpretation of GDPR provisions, one should reveal one's preference for one of the two concepts (or for a combination); in the best scenario, the decision to adopt one concept is justified and the other concept is criticized.

Advocate General Rantos did not comply with this postulate in the Opinion of 20 September 2022 (Case C-252/21); he used a preconceived position without giving reasons for that choice. The Opinion does not justify the thesis that the scope of application of Article 6(1)(b) GDPR must be handled as restrictively as possible in order to facilitate digital autonomy via Article 6(1)(a) GDPR. Several references are made to the views expressed in guidelines of the European Data Protection Board (EDPB). Anyone who reads these guidelines carefully must acknowledge that these guidelines adopt a data protection philosophy aimed at control without providing any justification or support for the adoption of such philosophy.

It is not certain that the Advocate General recognizes that he is using a specific preconceived understanding in approaching Article 6(1) GDPR, which itself is in need of discussion. More importantly, the Advocate General's approach does not meet the respective autonomous normative function of Article 6(1)(b) GDPR and Article 6(1)(a) GDPR. The efforts to marginalize Article 6(1)(b) GDPR are flawed in terms of data protection theory and data protection law.

III. Data protection law and private autonomy

The need to consider different choice architectures

Ultimately, allocating and delimiting Article 6(1)(a) GDPR and Article 6(1)(b) GDPR is an evaluation of different "choice architectures". Both provisions grant decision-making power to the data subject. Those who argue in favor of Article 6(1)(a) GDPR as the primary legal basis for data processing under data protection law are ultimately thinking in terms of the arbitrary freedom of the individual. If Article 6(1)(a) GDPR is applied in a contractual relationship between a service provider and its contractual partners, this means in specific terms that the contract only forms the background for the actual performance or counter-performance. Its practical

effectiveness ultimately does not depend (only) on the agreed aim of the contract but becomes dependent on a subsequent and arbitrary decision of the data subject. The service provider is required to take into account in the process of providing the service, whether consent to the use of personal data has been granted or denied and, moreover, whether it has been withdrawn or withdrawal is to be expected.

Without doubt, this results in the data subject gaining influence on the service to be provided. The service provider seems to be forced to individually tailor the service to cater for each data subject's decisions over the life-time of the contract. The process of providing the service in the contractual relationship is being dynamized and becomes uncertain over time because consent can be withdrawn at any time. What can be specifically offered becomes fluid and dependent on the fluctuations of the will of the data subject. This is undoubtedly an empowerment of the data subject, which can be interpreted as a gain in autonomy. So far, not enough thought has been given to whether it really makes sense to accept a continuous impairment of the legal relationships protected by Article 16 Charter in digital contractual relationships by establishing a subsequent and arbitrary right of constant revision by the data subject.

Arbitrariness as an impoverished conception of autonomy

Ultimately, however, this is a one-sided, possibly even impoverished, concept of autonomy. This is for several reasons.

Those who want to push back against Article 6(1)(b) GDPR and rely on Article 6(1)(a) GDPR in contractual relationships are trying to relativize and devalue contractual agreements. The agreement concluded between the service provider and its contractual partner is to be overlaid by further consent rights – irrespective of the question and without specific examination of whether what has been agreed is fair and reasonable. In substance, the service provider's contractual partners are thus infantilized – the ability to ensure fair and appropriate contractual terms on their own and to receive the service provided in accordance with the contract is generally denied to them.

The GDPR does not deprive a company of the right to define the digital service it wants to offer. This power is also protected under Article 16 Charter. If providing the service under the contract is put under the condition of obtaining consent, Article 6(1)(a) GDPR should not provide the data subject with more than a lever to bring about a termination of the contractual relationship. However, a data protection philosophy relying on arbitrariness just involves a negation of service and a return of the contracting parties to their earlier state where they were not bound to each other. It is regularly argued in favor of this concept of digital autonomy that this option will encourage companies to define and provide their service in such a way that data subjects do not make use of the right of withdrawal. One can see this as an expression of digital autonomy but should be aware that this is a specific and regressive understanding of autonomy. Also, the idea that a contract that is carried out with little use of personal data is always better than a contract that provides for extended use of such data is obviously incorrect as a general proposition.

Those who want to assign a right of consent to the contractual partner and data subject in the contract implementation process (Article 6(1)(a) GDPR) seem to be doing only good. However, this is not the case. Those who try to correct an existing digital contractual relationship by assigning consent rights also cause disadvantages. In the complex landscape of modern digital economies, where almost every provision of goods or services requires or entails data processing, requiring consent for every single data processing activity leads to fatigue and carelessness that undermines any supposed gain in autonomy. In the process of contract negotiations, it is possible for the data subject to seek and bindingly agree on contractual terms that the company might not offer if it had to factor in a withdrawal of consent at any time. As a matter of course, it depends on the specific circumstances of the individual case whether the service provider and its contractual partner will agree on contractual terms containing a performance that is more favorable to the contractual partner than it would be the case if the contract was carried out on the basis of Article 6(1)(a) GDPR. In any case, it is not excluded that the contractual partner who enters into a binding contractual agreement that involves the use of personal data receives a subjectively more valuable benefit than in a case where the service provider has to expect a withdrawal at any time. The key factor here is that the cost-benefit balance is so dependent on the situation and the individual case that it cannot be assumed that the allocation of rights under Article 6(1)(a) GDPR would always be in the interest of the data subject.

The blind insistence on arbitrary autonomy of the data subject/contract partner fails, moreover, to consider the public interest in innovation. If companies are required to develop services catering for a scenario where users can withdraw their consent at any time, this will massively hinder innovation for data-driven products. A dogmatic preference for Article 6(1)(a) over 6(1)(b) GDPR is already not possible for this reason alone.

Questioning of private autonomy under data protection law?

Those who adhere to a privacy philosophy emphasizing the value of arbitrary control are often inclined to dismiss the idea developed above of voluntary and equal shaping of social relations as insignificant or irrelevant. To some extent, one can also detect an underlying strategy of questioning or denying the use of private autonomy on the part of the data subject at all. This strategy was adopted by Advocate General *Rantos* in the Opinion of 20 September 2022. In his introductory remarks on the interpretation of Article 6(1) GDPR, he suggestively questions the relevance of the contractual commitment of the data subject and whether it was freely given: the processing takes place “on the basis of the general conditions of contract imposed by the controller, in the absence of the consent of the data subject, or even against his or her will” (para. 51). He also ignores the fact that digital consumer contract law ensures that nothing can be agreed in digital contracts that would result in an unreasonable burden on consumers. The assertion that something would be stipulated in a validly concluded contract “against the will” of the contracting parties goes against the very core of European contract law. It may serve populist prejudices but should not appear in a legal document of the European Court of Justice.

Probably the most important argument against the point of view expressed by Advocate General *Rantos* goes back to the foundations of Western liberal legal thinking. Ethics, law and politics are based on the axiom that human self-determination is expressed not least in freely entered, fairly negotiated contractual agreements that are not unreasonable in content. This gives rise to obligations, but also to benefits that are in line with the subjective preferences of the contracting parties. No one would think of adding an arbitrary right of consent at the performance level to non-digital contracts. There is no reason why this should be fundamentally different in the area of digital content contracts. It must be a concern of the EU and the Member States to ensure that the legal framework necessary to ensure the fairness and adequacy of contractual arrangements involving digital content is put in place. Respect for digital autonomy in this context implies that there must be sufficient leeway for contractual arrangements that allow contracting parties to balance their respective interests in the digital society. Paternalism and guardianship must be avoided – the ideas of the good life and the models of life will be as diverse in the digital society as they are in the real world. The occasionally observed idea that everything is different in digital contractual relationships is misguided; it cannot be justified in terms of data protection law either. The ability and the will of people acting in a self-determined manner to be able to enter into binding contracts involving digital content would ultimately be called into question if one were to take the position that autonomy at the level of performance presupposes an arbitrary possibility to unilaterally amend a contractual relationship. Individuals are infantilized by this paternalistic view, as has already been said above. Instead, companies must be enabled to keep the option of promising more (in terms of performance) for the certainty of being able to contractually dispose of data (lit. b) than if a processing is based on lit. a); a data subject who agrees to this does not forfeit but realizes autonomy.

The relative value of the authorization that lies in the application of Article 6(1)(a) GDPR can therefore only be meaningfully determined if it is taken into account that contractual agreements can be a manifestation of the digital autonomy in the digital economy. If digital autonomy results in entering into contractual agreements and is justified under data protection law on the basis of Article 6(1)(b) GDPR, individuals are indeed deprived of a right to arbitrariness. However, in this way they are taken seriously as legal subjects.

No review of the content of contracts under data protection law

This leads to the conclusion that data protection law cannot control the content of effectively concluded civil law contracts. Repeatedly, one can observe the attempt to make Article 6(1)(b) GDPR an instrument under which a content assessment of digital contracts can be carried out, not least in the view expressed in the already mentioned EDPB guidelines. This is also reflected in Advocate General *Rantos*' opinion. In his view, "bad" contracts are to be sanctioned by applying the consent requirement at the implementation level (para. 56 with paternalistic considerations on the benefit calculation of the data subjects). His opinion is not only based on the thesis that the judicial or administrative review of necessity in Article 6(1)(b) GDPR is not only about the question whether the undertaking's data processing proves to be

necessary for the *performance of what has been contractually agreed*. On the basis of Article 6(1)(b) GDPR, he also intends to control the content of the contract itself in terms of data protection law. According to this view, a contractual agreement that is not based on a literal interpretation of the principle of data minimization may be not invalid under civil law (this is clearly beyond the scope of the GDPR); however, it is not intended to fall under Article 6(1)(b) GDPR and cannot serve as a justification for data processing even if both parties consider it to be mutually fair.

IV. Consequences for the interpretation of Article 6(1) GDPR

This has direct consequences for the interpretation and application of Article 6(1) GDPR.

First, it would be manifestly wrong to assume that the digital autonomy of individuals in contractual relationships can always be optimized by applying Article 6(1)(a) GDPR. Depending on the facts of the case and personal preferences, it is more in line with the interest of a data subject to conclude a contract that (also) extends to the use of personal data and that is treated in accordance with Article 6(1)(b) GDPR. This applies in any case if the service provider wants to reliably design digital services whose content has been made the subject of a contract valid under consumer protection law by the company and the contractual partners. Neither side is served in the long term if the company must always fear that contractual partners may withdraw their consent and force the company to offer another service that does not fully meet its needs and those of the data subject. Efforts to apply Article 6(1)(a) GDPR in digital contractual relationships would involve the risk of hampering the ability to innovate and improve services and products, even if this is precisely what parties, in particular the service provider but also data subjects, want.

Secondly, it would be completely pointless to rank Article 6(1)(b) GDPR and Article 6(1)(a) GDPR by order of philosophical preference without considering that the digital contract law of the EU and the EU Member States ensures that digital contracts can only be concluded effectively if (both procedurally and in terms of content) certain minimum requirements regarding level of information, fairness and equivalence are met. It would be narrow and myopic to approach Article 6(1) GDPR ignoring that digital contract law sets a framework that includes autonomy-securing fairness and adequacy provisions, and that the contracting parties, obviously each from their own subjective viewpoint, have determined that there is sufficient value for them in what was agreed. If it is ensured under contract law that the contract concluded between the company and the data subject is transparent and provides for a fair exchange of performance and consideration, there is no reason to grant the data subject another right of consent under Article 6(1)(a) GDPR for the performance of the contract. On the contrary, those who advocate an additional requirement of consent rather destroy the very material reciprocity of the bargain struck between the parties, the definition of which is made possible and secured by contract law. In the considerations of Advocate General *Rantos*, this connection between digital contract law and data protection law is completely ignored.

Therefore, thirdly, there is ample reason to take Article 6(1)(b) GDPR in the literal sense. This provision does not allow for any data protection control of the contract concluded between the company and the data subject but links the legal justification solely to the fact that no more data than necessary is processed for the performance of what has been agreed in the contract. It is not the subject matter of Article 6(1)(b) GDPR to distinguish good contracts from bad contracts. Therefore, under Article 6(1)(b) GDPR the legal justification does not depend on the fact that a contract has been entered into between the two contracting parties which is “good” (according to whatever criteria). Article 6(1)(b) GDPR does not provide a starting point to protect people who have freely and on an informed basis entered into a contract that they consider to be beneficial for themselves. This provision prevents data from being processed beyond what is contractually agreed (“necessary”); but it does not provide for EU civil servants to ascribe to themselves the right to judge and override people’s benefit calculations. In short, adequate data protection does not mean paternalistic intervention as to individual preferences reflected in a mutually agreed contract. As an aside, it should be recalled that the GDPR provides a comprehensive system of protections even if Article 6(1)(b) GDPR is chosen as legal basis; this system ensures the adequacy of data processing in a variety of ways that meet the requirements of Article 8 Charter.

This results – fourthly – in the imperative necessity of clearly distinguishing between three levels when applying the necessity criterion under Article 6(1)(b) GDPR.

1. It is *not* the subject of the necessity test under data protection law whether a service provider *could* have agreed on a different service with its contractual partners, nor whether it has previously provided a different service. In particular, the necessity test provided for in Article 6(1)(b) GDPR does not include the question of whether a service provider that has concluded a contract with its contractual partners for personalized services could perhaps also have concluded a contract for non-personalized services. Such control of the contractual terms is not legally possible even if it could be demonstrated that less personal data is processed when performing a non-personalized service. Data protection law does not contain a substantive benchmark that could support a meaningfully reasoned decision on this issue. Those who advocate this approach only introduce subjective preferences – such as the view that non-personalized advertising is always better than personalized advertising. If the data subject has taken the informed and free position that the concluded contract reflects his or her preferences, there is no reason to correct this under data protection law. If there are doubts as to whether a fair contract has been concluded, this must be resolved under contract law.
2. The necessity test pursuant to Article 6(1)(b) GDPR cannot be used as a lever to induce a company to deviate from what has been contractually agreed in the process of performing the contract. If the contract between the company and the contractual partner provides for the provision of a personalized service that can be performed in accordance with the contract by processing personal data, it cannot be argued under data protection law that the company could also provide a different service (in deviation from the contract).

3. The necessity test under Article 6(1)(b) GDPR solely covers the examination of whether the company collects or uses data in the process of providing the service that is not necessary to perform the contractually agreed subject matter of the service. In this regard, necessity is then a legal concept of Union law; and in this regard, the decision can of course not remain at the discretion of the company but must instead be based on “objective” circumstances. In short, anyone who confuses issues of determination and definition of the contractual performance with the provision of performance will fail to meet the legal requirements for the application of the necessity criterion, from the outset.

Fifthly, it follows from the above that the legal policy assumption that the data subject could (or even must) be given a *de facto* right to determine entrepreneurial performance through the application of Article 6(1)(a) GDPR would be wrong. Data protection law does not interfere with the entrepreneurial right to determine service provision and performance. Nor does it take precedence over other EU objectives, such as ensuring EU competitiveness, the innovative strength of companies in the EU internal market or the fundamental right under Article 16 Charter (GDPR, Recital 4). A company has the freedom to enter the market with a service offering that is solely and exclusively personalized services. Data subjects then have the option to accept that offer or not. They have no right to adaptation and to unilaterally change the terms of service, for example in the direction of data minimization. In particular, Article 6(1) GDPR does not contain any lever that can be used to force companies offering a personalized service on the market to switch to a non-personalized service under data protection law.

V. The basis of the digital economy must be the binding digital content contract

EU data protection law is currently faced with the challenge of extricating itself from a one-dimensional world of ideas according to which the consent requirement under Article 6(1)(a) always optimizes people’s digital autonomy. It is easy to demonstrate that in contractual relationships the application of Article 6(1)(a) GDPR can actually result in a *loss* of autonomy in the sense that certain agreements can no longer be concluded. The protection objective of Article 8(1) Charter will not be achieved if it is not considered that Article 6(1)(b) GDPR and Article 6(1)(a) GDPR each entail different “choice architectures”. The simplistic thesis that a normative hierarchy is built into the legal basis of Article 6(1) GDPR, at the top of which is Article 6(1)(a) GDPR, must be rejected. It is necessary to recognize the independent value of Article 6(1)(b) GDPR. Were the authors of the GDPR smarter than its current interpreters?

The digital age began twenty years ago now. It seems that digital transformation has recently accelerated further. Digital manifestations are appearing in more and more areas of life, and more and more contractual relationships are extending to digital content. So far, it is not even possible to discern in vague outlines what the future digital society will look like. The resulting demands on legal policy are enormous: regulation in the dark is just as unfeasible as naïve belief in progress or

fatalistic inaction. One of the main concerns of law and politics must be to ensure that people are able to lead a self-determined and good life in the emerging digital society. The path to the digital future must not lead to a state in which people lose autonomous self-determination in digital life. At the same time, law and policy must ensure that a competitive and innovative economy is created and maintained, even in the new environment shaped by data economics. Only competition and innovation can effectively serve the preferences of people in the digital society; without it, maintaining the level of prosperity achieved in the EU will be impossible. Talking about digital autonomy without having the requirements of a functioning economy in mind is at best myopic, at worst even pointless.

In his Opinion of 6 October 2022, Advocate General *Campos Sánches-Bordona* expressed the need to be forward-looking and emphasized the importance of protecting EU competitiveness and innovation. He has placed data protection law in a wider context and avoided any myopic approach. His Opinion stands for a forward-looking interpretation of data protection law.

Author's note: The author holds the Chair of Constitutional and Administrative Law, European Law and International Law at the Faculty of Law of the University of Tübingen. He advised Meta Platforms, Inc. (formerly Facebook, Inc.) in 2019 on the question of the relationship between the powers of data protection authorities (Articles 51-66 GDPR) and competition authorities (Section 19 GWB) (Questions referred 1 and 7 in Case C-252/21).
