APRIL 6
2024

Weekend EU LAW LIVE Edition

stay alert | keep smart

Nº181

MARTIN NETTESHEIM

EU DATA PROTECTION LAW AND PAY-OR-CONSENT BUSINESS MODELS

EU Data Protection Law and Pay-or-Consent Business Models

Martin Nettesheim [1]

I. Data protection law at a crossroads

Alarmist tones are currently being heard from the European data protection authorities. European data protection law is said to be currently facing a 'huge fork in the road'.[2] Even if one does not follow the excitement, it is easy to see that the authorities are faced with an important decision. The restrictive interpretation of European Data Protection law and new digital regulation advocated by the European data protection authorities and the European Data Protection Board ('EDPB') required the digital company *Meta* (as others before) to deploy a 'Pay or Consent' model in order to ensure freely given and valid consent and at the same time safeguard the viability of its business model. As from November 2023, *Meta* has no longer offered the social network service *Facebook* free of charge exclusively, but has also offered a parallel pay model that provides for a monetary price for the use of the social network service, eliminates the use of data for advertising, and will therefore not show advertisements. The introduction of this model has resulted in European data protection authorities raising questions that go to the heart of data protection law, its teleological core concern and essence.

The introduction of the 'Pay or Consent' model has resulted in European data protection authorities raising questions that go to the heart of data protection law, its teleological core concern and essence

1. Professor of Constitutional Law and EU Law at the University of Tübingen Law School (www.nettesheim.org). Currently, he also serves as the president of the German Association of Professors of Public Law (www.staatsrechtslehrer.de). He has advised both the German Federal Parliament (Bundestag) and the German Federal Government on questions of constitutional and EU law. The article builds on an examination of Art. 6 (1) GDPR, available here (updated version currently in print (Lexxion Publishers)).

2. This is the assessment of the Norwegian Data Protection Commissioner, available here.

How can Meta's business decision force data protection law to clarify its nature? The GDPR[3] stipulates that the data protection consent that authorises a controller to process data (Article 6(1)(a) GDPR) must be freely given (Article 4(11) GDPR). Article 7(4) GDPR, the ambiguity of which reflects differences of opinion in the legislative process, stipulates that the assessment of this requirement of voluntariness of consent in a horizontal contractual relationship between the controller and the user depends, among other things, on whether the processed data is necessary for the fulfilment of the contract ('prohibition of tying'). Recital 42(5) GDPR also stipulates that consent can only be assumed to be freely given if the data subject 'has a genuine or free choice' and is able 'to refuse or withdraw consent without suffering detriment'. In a recent judgment of 4 July 2023 in *Meta/Bundeskartellamt*, the Court of Justice has established that the characteristic of 'genuine or free choice' of the options offered by a company processing data as a controller forms part of the voluntariness dogma of Article 6 (1)(a) GDPR in conjunction with Article 4(11) GDPR, at least where it has a dominant market position.[4]

In *Meta/Bundeskartellamt*, the Court of Justice ruled that a company with a dominant market position can obtain consent under data protection law that is free, i.e. fulfils the criterion of voluntariness (para. 147). However, depending on its particular market power, it must offer its users 'an equivalent alternative' to a business model based on the collection and use of personal data (in particular for advertising purposes) in order to guarantee voluntariness. This equivalent alternative, 'which does not involve such data processing operations', can be offered 'where appropriate, for a reasonable fee' (para. 150). For the Court, the concept of 'genuine or free choice' thus centres on the possibility of choosing between different but equivalent service offers.[5]

In November 2023, this judgment (along with the requirements of the Digital Markets Act)[6] prompted *Meta* to expand its business offering so that a pay model and an advertising-financed model based on consent to the collection and use of personal data for personalised advertising purposes will be applied side by side. The company guarantees the right to 'genuine or free choice' under data protection law by giving users and data subjects the choice between two offers – a more data-use intensive but monetarily free model on the one hand and a less data-use intensive but fee-based model on the other. In particular, the fee-based option entails that no advertising personalisation takes place at all. However, this step has not brought peace in terms of data protection policy. Data protection activists say that the future of digital privacy is 'hanging in the balance'.[7]

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p.1, (the 'GDPR').

4. Judgment of 4 July 2023, C-252/21, *Meta Platforms Inc. and others v Bundeskartellamt*, EU:C:2023:537, para. 148. On the position of the European Data Protection Board: EDPB, Guidelines 5/2020 on consent under Regulation 2016/679, 4 May 2020.

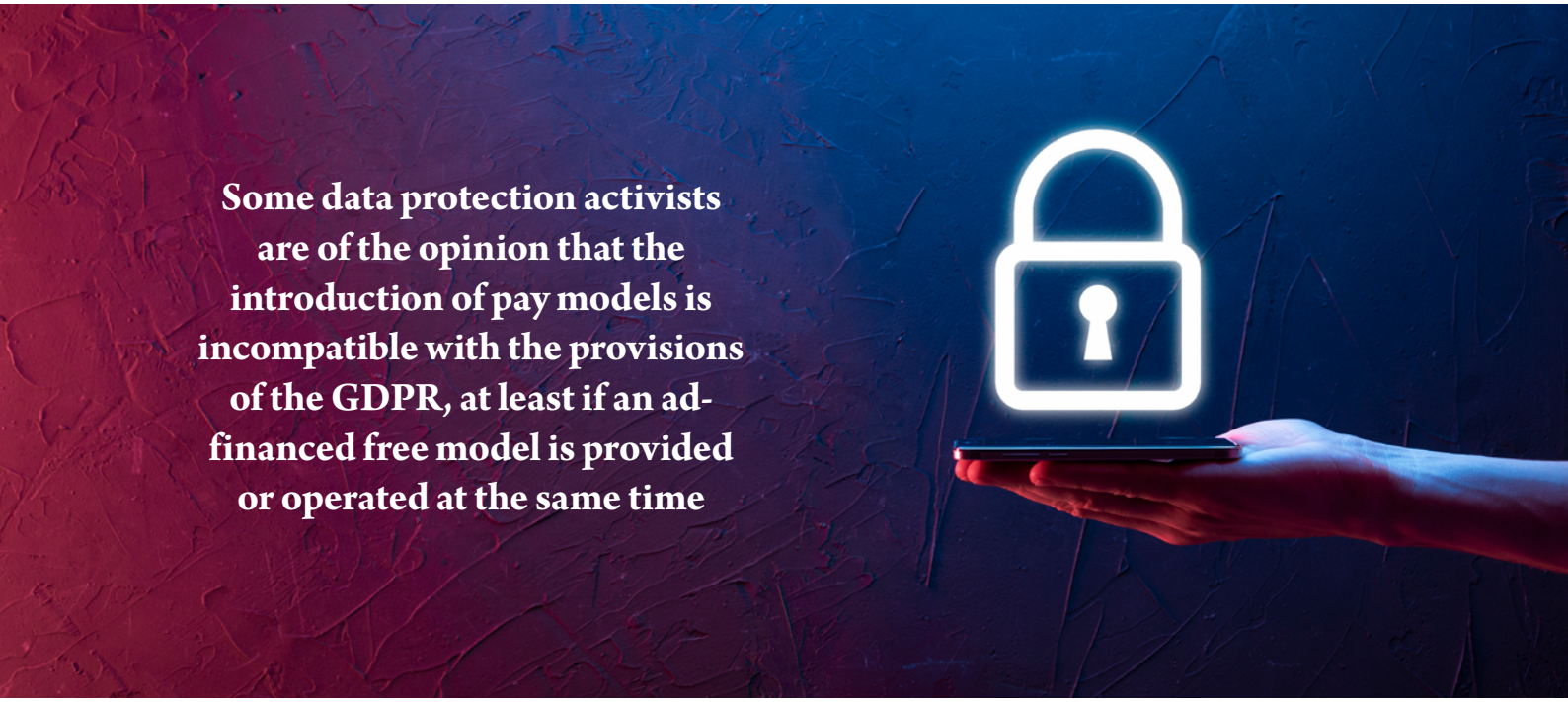
5. The Court of Justice has thus –rightly– decided against an interpretation of the GDPR according to which the company must provide the same service to users who refuse consent as to those who give consent. The view that the GDPR establishes an obligation to contract in the event that consent under data protection law is refused or withdrawn has no basis either in the text of the GDPR or in its history; it also does not correspond to its purpose.

6. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, p. 1.

7. See here.

II. A 'social justice turn' in EU data protection law?

The compatibility of 'pay or consent' models[8] with the provisions of the GDPR[9] is viewed differently by commentators. In many cases, the introduction of such models is seen as a benefit for data protection – on the one hand, because it allows users to switch to data-minimalist offers, and, on the other hand, because it makes it clear that the free alternative also has a 'price'.[10] Some European data protection authorities explicitly consider 'pay or consent' models to be permissible, but others raise some concerns. A group of data protection authorities[11] recently approached the EDPB in order to obtain a data protection assessment of 'pay or consent' business models. The EDPB has a deadline of eight weeks in accordance with Article 64(2) GDPR; this deadline can be extended by six weeks, which would appear to take us to a deadline in early May at the very latest. The timeframe is tight and may not do justice to the significance that the requested decision will have for the future of data protection and digital business models in the European Union.



8. The phrase 'Pay or Ok' is also used in some cases.

9. The EU Commission has initiatied an inquiry into "pay or consent"-models under the DMA (see https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689).

10. Only recently there have been calls to introduce pay models in order to improve data protection (See Kerber et al. Study for the consumer advice centre, available here).

11. These are the authorities of the Netherlands, Norway and Hamburg. The application was received by the EDPB on 25 January 2024.

Resolute and vocal opposition to the introduction of monetised alternative service offerings comes from a rather surprising quarter. Some data protection activists are of the opinion that the introduction of pay models is incompatible with the provisions of the GDPR, at least if an ad-financed free model is provided or operated at the same time. At first, it sounds like a silly joke when one hears that the decision of a large digital company to introduce a data-minimalist service that eliminates the tracking for personalised advertising is being attacked by data protection NGOs and activists. Indeed, one is inclined to believe that there has been a misunderstanding when one learns that EU data protection law is to be used against the introduction of data-minimalist business models. The distorted logic of such political moves becomes clear when one takes a closer look at the arguments put forward and realises that data protection law is to be charged with protective purposes and concerns that lie far beyond the protection of digital autonomy and privacy.

The NGOs behind this movement argue that fee-based access to media content and social networks is socially unfair and contrary to equality. They argue that an end to the 'free' culture would lead to personal economic hardship and possibly even bankruptcy, social exclusion and political voicelessness for many people. The transition to a world in which media offerings and business services such as social networks must always be paid for ('pay model') would result in the commercialisation of the right to informational self-determination. In future, the extent of privacy and data protection would depend on the willingness and ability to pay, and data protection would become a right of the rich. The introduction of prices for business services is compared by these NGOs to the introduction of a price for exercising the democratic right to vote. In essence, the aim is to turn data protection law into an instrument that can be used to pursue socio-political goals. Socio-political concerns ('social justice') are to take the place of only safeguarding digital autonomy and privacy.

But the NGOs go even further. They don't just want to replace a protection goal that focuses on digital autonomy and privacy with a much broader, vague and easily manipulated protective approach aimed at achieving social justice. They also want to declare this approach to be absolute, with the result that opposing protection concerns and other legitimate interests at stake (including the fundamental right to conduct a business) cannot come into play. Proponents of this approach close their eyes to the fact that without pay or consent models, many providers of digital services or content may only resort to subscriptions as only means to finance their services and therefore paywalls would start dominating. This would have the exact opposite effect of promoting a 'free' culture.

III. The alternative: valorisation of data or limitation of the protective approach of EU data protection law

Against this background, it becomes clear why some of the European data protection authorities are talking about being at a crossroads. It is not entirely wrong to see these authorities confronted with an almost tragic decision-making situation.

The data protection authorities would only be able to make a comprehensive comparison of the economic 'equivalence' of the pay model (monetary costs, but gain in privacy) with the consent model (no monetary costs, but consent to the processing of personal data for personalised ads) if they were to abandon the alleged dogma

that the GDPR does not permit the treatment of personal data as marketable goods and their valorisation.[12] They could then assess the equivalence of the services by comparing the monetary price of the service in the pay model with the utility or market value of the data collected in the consent model. The data protection authorities would gain a (data protection) legal lever with which they could carry out comprehensive monitoring of the new 'pay-or-consent' business model on the basis of market fairness. However, the theoretical and idealistic price would be high: the data protection authorities would then also be forced to classify personal data as marketable goods, to no longer categorically deny the existence of data markets and to recognise the interests of the data subjects in the economic exploitation of their data.

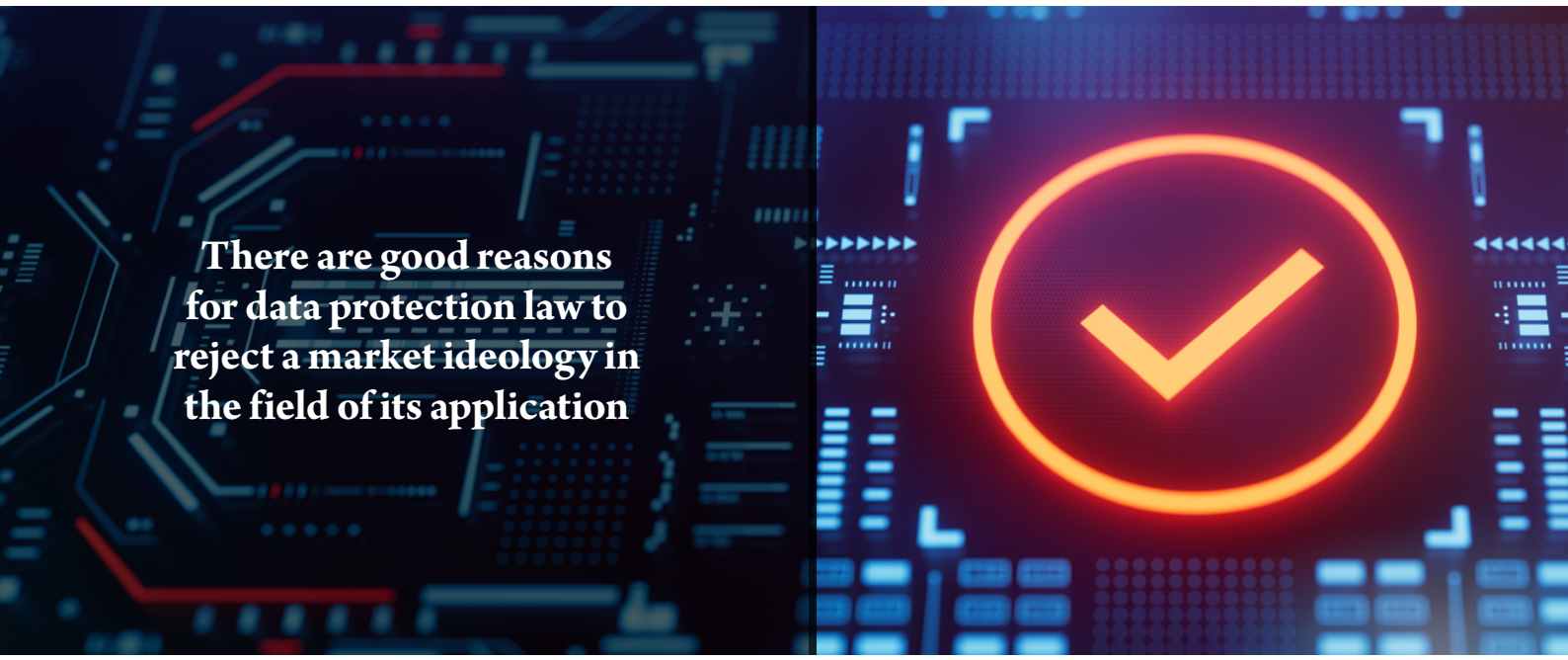
The data protection authorities would only be able to make a comprehensive comparison of the economic 'equivalence' of the pay model with the consent model if they were to abandon the alleged dogma that the GDPR does not permit the treatment of personal data as marketable goods and their valorisation

If, on the other hand, the data protection authorities were to stick to the dogma that personal data cannot be valorised, they would not be able to consider the economic value of personal data and compare the equivalence of pay models and consent models through the lens of a standard of market fairness. Their scrutiny of Meta's new business model would have to be limited to the question of how the pay model relates to the consent model with regard to the specific data protection objectives (digital autonomy and protection of privacy). They would have to restrict their approach to the question that the EDPB decision was focused on, i.e., the legal basis for the processing of personal data for personalised ads, enlightened by the Court of Justice.[13] Further protection goals (market contestability, prevention of financial exploitation, etc.) would have to be pursued by the competition and consumer protection authorities, also within the scope of their specific remit. The social security law of the EU Member States would ensure, through financial support, that all persons are in the position to take advantage of the pay models, thus ensuring 'genuine or free choice'.

12. Opinion 4/2017 of the European Data Protection Supervisor on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, of 14 March 2017, (denouncing the scenario 'that people can pay with their data in the same way as they do with money'). A summary is available at OJ 2017 C 200, p. 10.

13. The DMA explicitly mentions equivalence (Recital 36).

The alternative outlined above must not be misunderstood. The EU legislator[14] and academic data science studies (both in economics, social sciences and law) assume that data must be understood as valuable goods on the market. However, there is no reason for data protection law to adopt this construction of social reality and identify with this pattern of meaning. On the contrary: there are good reasons for data protection law to reject a market ideology in the field of its application.



IV. 'Power paradigm' and 'harm paradigm'

Many of the contributions to the discussion that are currently being made on the question of how to categorise 'pay or consent' models under data protection law have no depth in terms of data protection theory or teleology. An in-depth discussion of the problem requires an argument based on data protection theory. It makes sense to analyse 'pay or consent' models against the background of the two basic paradigms of data protection law behind the specific provisions of the GDPR: the 'power paradigm', according to which data protection law serves to *empower data subjects*, and the 'harm paradigm', according to which data protection law serves to combat *threats and harm in the area of personal privacy.* Both paradigms are fundamentally complementary and complement each other; however, as will be shown below, they can also come into conflict.

14. Digital Content Directive 2019/770 (Recital 24, Art 3(1)) (OJ 2019 L 136, p. 1) and the Consumer rights Omnibus Directive 2019/2161 (OJ 2019 L 328, p. 7) expressly mention that a service can be provided in consideration of the provision and use of personal data. In addition, the Data Governance Act (Regulation 2022/868, OJ 2022 L 152, p. 1) goes a step further by setting out the framework for individuals to commercialize their own personal data.

1. Data protection law as empowerment

The first and most important teleological purpose of data protection law is the *empowerment of data subjects.* Data protection law enables people to exercise control over the personal information that is available about them in the social spaces in which they are active (*control of the information environment*). To this end, the GDPR provides them with legal means to control the collection, processing and use of personal data (privacy-related or not).[15] This power of control is established above all by the prohibition with reservation of authorisation and the right of consent (as well as other legal bases) set out in Article 6 GDPR.[16] The empowerment approach is neutral as to the way a data subject uses its control power: Anyone who releases personal data for collection and use through consent exercises this power of control in the same way as someone who refuses consent. The 'power paradigm' under data protection law can therefore raise no objections to the decision of the data subject to commercialise their data, as long as the consent in this regard is truly self-determined (sufficient information and transparency, no external duress, etc.). On the other hand, this paradigm provides a particular reason to ask in horizontal contractual relationships between companies and consumers whether structural circumstances turn the exercise of the right of consent into an act of merely formal self-determination. This could be the case in contractual relationships with the provider of an 'essential facility',[17] but not, as the Court of Justice rightly emphasises, where a company merely has a dominant market position.

If data protection law is understood as an instrument of empowerment, the evaluation and assessment of 'pay or consent' models results in the following: In principle, if the data subject is given the option of choosing between a monetarily priced service that is provided without the processing of personal data for ads and an unpriced service that is associated with the processing of personal data for ads, it benefits from a *gain* in digital autonomy. This applies in both directions: if a company that has previously financed its service through personalised advertising now offers a pay model, the gain in digital self-determination lies in being in a better position in terms of privacy interests in the future. If a company that has so far financed its services via a monetary price were to add a service financed via personalised advertising, the empowering effect would be that the data subject could now use their data to 'pay'.

However, empowerment would not occur if the alternative offer was too disadvantageous so that it did not entail any expansion of individual options for action on the basis of a material concept of autonomy. A pay model cannot entail genuine empowerment if the price demanded is so high that it is beyond the *financial capacity of the average user*. Anyone who is given the option to make use of a pay model but decides against it due to a lack of *willingness*

15. Accordingly, the concept of privacy refers to the type and scope of control over personal information. The control can relate to various factors (subject of an authorisation to obtain, use or exploit information; type of information; purposes of the authorisation to use or exploit, etc.).

16. Article 6 (1)(c) to (f) GDPR makes it clear that the power of control is not unlimited.

17. Obviously, Meta services are not essential services. This is not even claimed by progressive data protection activists. Moreover, even in the case of an essential facility, the competition rules do not conclude that a company is obliged to provide a service for free and that the taxpayers assume all or part of the price. To name just a couple of examples: all of us (individually) pay for electricity and water.

to pay or *for reasons of preference* has been offered a genuine alternative, has then made a self-determined decision, and has thus been empowered. It would therefore obviously be wrong from a data protection law perspective to ignore the difference between the data subjects' ability and willingness to pay.[18] It would also be wrong to question the empowering effect of a pay model by pointing out that people prefer to spend their money differently – the realisation of preferences is an expression of exercised autonomy, not a curtailment of it.[19]

The reference to the financial capacity of the 'average user' here is important, because in order to assess whether the provision of a pay model constitutes genuine empowerment for the possible users, data protection law must make a generalised assessment. It cannot consider the circumstances of each specific user, because this would result in the abandonment of the normative generality of European data protection law. The general application of laws such as the GDPR is not only a practical necessity (how could each case be treated individually?), but also an expression of a normative ideal of equality before the law. To be clear: The concern that the introduction of a pay model could lead to discrimination and social or political exclusion of a minority of users must be taken seriously. However, it would be a conceptional mistake and an abuse of data protection law to use it as an instrument to achieve social justice. EU data protection law is not an instrument, with which a differentiating social policy could be pursued. Those who take these concerns seriously will not call for remedies under data protection law, but will argue in favour of EU Member State's social support covering access to the services deemed politically and socially necessary. It is the task of the general social security system of the EU Member States to react to any injustices resulting from the economic situation of the potential users of digital services, particularly with regard to the goal of giving everyone access to media offerings or social networks, provided that it should be one the EU Member States should be concerned with. None of the statements by data protection activists fighting for a 'social justice turn' in data protection law even mentions the fact that there is another area of law for achieving these goals.

A pay model cannot entail genuine empowerment if the price demanded is so high that it is beyond the *financial capacity of the average user*

18. For example: C. Carugati, 'The "pay-or-consent" challenge for platform regulators', Bruegel analysis, 32/2023, 6 November 2023.

19. In the opposite case (a company places a consent model alongside the pay model), digital authorisation *always* occurs. However, this scenario can give rise to problems of 'digital harms' (see below).

EU data protection law is not an instrument, with which a differentiating social policy could be pursued

What follows from these considerations in terms of legal doctrine? Anyone who understands data protection law as an instrument of empowerment will not relate the criterion of 'equivalence' of the pay model and the consent model (as options that open up autonomy) to market prices and market justice. It would be a misconception to assume that data protection law utilises (or must utilise) a market ideology that can only consider everything according to criteria of economic utility and market price. What matters for data protection law is the gain of autonomy or self-determination (legal power) in the handling of personal data. If the pay model introduced later and offered as an alternative to a consent model brings more or different benefits in this respect than the previous model, it must be regarded as 'equivalent'. A pay model that offers the option of better privacy protection and is not beyond the data subjects' financial capacity is therefore always 'equivalent'.

Consequently, EU data protection law should not even begin to make an economic comparison between the monetary costs of a pay model and the economic value of the data used in a consent model for the placement of personalised advertising. A further examination of questions of the utility or market value of data and the market fairness of the two exchange relationships would change the nature of data protection law in a harmful way: an instrument for the protection of personal self-determination would become an instrument for the implementation of a certain market ideology.

2. Data protection law as an instrument for defence against privacy risks and damage

Data protection law can also be understood as an instrument to combat risks and harm in the sphere of digital privacy of data subjects. It is obvious and requires no further explanation that entering into a social relationship with another actor always entails a loss of privacy. This also necessarily applies in the event that an individual enters into a business relationship with a company in order to receive its services. In a liberal society, it is fundamentally the competence and responsibility of the individuals to decide for themselves whether, when establishing horizontal private law relationships, the give and take in the reciprocal relationship corresponds to their own benefit calculation. This also applies to the costs of privacy incurred in this relationship. In principle, paternalistically patronising people in their assessment of the costs of privacy is unacceptable.

In this context, however, the GDPR is not content with a purely formal concept of autonomy based on the external act of declaring one's will. It aims to ensure an informed and rational decision by the data subject under conditions of transparency and sufficient predictability of the consequences of one's decision. Data protection law therefore rightly assumes that the privacy interests of a person can be impaired or damaged if consent is not an expression of a decision that meets these criteria of material autonomy. Furthermore, it is conceivable that data protection law protects certain spheres of privacy even against the will of the data subject – for example, by an unqualified prohibition of the commercial use of certain types of personal data (or for other overriding reasons provided in Article 6(1) GDPR). It depends on the context and is ultimately an expression of the political will of the legislator as to whether and where privacy should also be protected against the will of the individual. Such legislative will cannot be replaced by the exercise of political discretion of data protection authorities. The concern to protect privacy can come into conflict with the empowerment concern of data protection law insofar as there may be cases in which data subjects are prevented from commercializing their data (empowerment) for overriding reasons of privacy protection.

For the classification of 'pay or consent' under data protection law, this means that the privacy costs that arise on the part of the 'consent' model are relevant under data protection law. If a company that previously relied entirely on a pay model introduces a model with consent elements alongside it (example: an insurance company that offers a rate reduction in the event that the policyholder allows their behaviour to be monitored), the resulting privacy costs must be taken into account when assessing whether this is a genuine case of free consent. If, on the other hand, a company introduces a data-minimalist pay model alongside a 'consent' model, no privacy risks arise that could give data protection law cause to intervene. To put it very simply and directly: if a digital company supplements its existing consent model with a new data-minimalist pay model, there is absolutely no new risk to the privacy of potential users.

For the classification of 'pay or consent' under data protection law, this means that the privacy costs that arise on the part of the 'consent' model are relevant under data protection law

What does this mean with regard to the doctrinal concept of 'equivalence' of alternatives in data protection law? While data protection law must map risks and damages in the area of personal privacy, it cannot cover the financial interests of the data subject. The doctrinal concept of 'equivalence' must compare the alternatives offered by the company, but it cannot take into account any financial disadvantage resulting from the need to pay a monetary price. The fact that the pay model establishes a monetary payment burden lies outside the protective purpose of data protection law.

The above considerations make it clear that 'pay or consent' models certainly raise data protection issues with regard to the defence against privacy risks. However, this does not apply in the event that a data-minimalist pay model is introduced alongside a 'consent' model. In this case, there is no impairment of privacy interests from the outset.

3. No protective 'paradigm' beyond empowerment and information privacy

It is important to emphasise that data protection law pursues two protection goals that are on equal footing: the goal of empowerment and the goal of protecting personal spheres of privacy. In contrast, European data protection law does not recognise any further protection concerns, such as the protection of the financial interests of market actors, the establishment of free access to business services or 'social justice'. The EU data protection authorities would misunderstand the meaning of the GDPR and overuse their legitimacy as independent administrative authorities if they tried to replace the two protection objectives contained in the GDPR with additional political concerns not approved by the EU legislature.

V. Conclusion: pay or consent models can raise data protection issues, but do not necessarily have to do so

The above considerations make it clear that the 'equivalence' criterion used by the Court of Justice in its *Meta/Bundeskartellamt* judgment must be interpreted through the lens of the protective purposes of EU data protection law. The criterion must be given a specific meaning under data protection law. It would be normatively wrong to tear the criterion out of its normative context. As a matter of legal methodology, the interpretation and application of the criterion must be guided by the fact it deals with the specific equivalence of the alternatives offered by the company *evaluated on the basis the interests of the EU citizens as data subjects*. On the other hand, an evaluation based on the interests of EU citizens as market citizens with financial interests would be misguided.

The 'equivalence' criterion used by the Court of Justice in its *Meta/Bundeskartellamt* judgment must be interpreted through the lens of the protective purposes of EU data protection law

It is in line with the protective purpose of data protection law if data protection law empowers the data subjects and intervenes against privacy risks. If 'pay or consent' models are evaluated through the lens of the empowerment paradigm, they are always and without limitation a win for the data subject. This would only not be the case if the monetary price for the pay model were so high that it exceeded the average user's ability to pay. If, on the other hand, one takes the 'harm' paradigm as an evaluative standard, there is reason for differentiation: the introduction of a consent model alongside an existing pay model can give rise to data protection intervention if the privacy costs are too high. In contrast, in the opposite case there is no approach to data protection concerns.

To conclude: Data protection authorities are not called upon to deal with the protection of people's financial interests. Data protection law is also not an instrument with which the unwillingness of recipients of a business service to pay can be legally protected. Social policy concerns are of course relevant in digital markets; however, they cannot be made the subject of EU data protection law via the doctrinal characteristic of the concept of 'equivalence'. Instead, they must be pursued under social security law and be addressed by EU Member state social security administrations. It cannot be the concern of data protection law to process general considerations of 'social justice'. Calls for a 'social justice turn' of EU data protection law are unwarranted.

Subscription prices are available upon request. Please contact our sales department for further information at

subscriptions@eulawlive.com

ISSN

EU Law Live **2695-9585**
EU Law Live Weekend Edition **2695-9593**

www.eulawlive.com