Privacy and Data Protection (JUS 5630)

Spring 2021

Exam question: guidance notes

[**Overall remarks:** A major challenge presented by this exam is that students were only permitted to write an answer with a maximum of 3,000 words and yet the exam raises quite a large number of issues. Tackling each of these issues in depth would easily exceed the word limit, so students' treatment of them (or at least some of them) will necessarily be superficial. Students were informed prior to the exam that they ought to be very concise in their answers. They may use bullet-points if necessary, also for the 'essay' style part of the exam (question 5). Accordingly, brevity or use of bullet-points should not be penalized.

It is also important to note that, due to the pandemic, all teaching at the Faculty of Law has been carried out online in the Spring semester 2021 and access to student reading rooms has been subject to significant restrictions. As the pandemic has made the study situation extremely demanding, grading must take this into account.

In respect of referencing, it is up to students themselves to adopt a suitable system; there is no particular template they must follow, nor is there a requirement that students include a bibliography at the end of their exam paper. Moreover, students are expected to be able to answer the exam questions on the basis of the reading materials listed as pensum (both required and recommended reading), lecture handouts, and case law referenced in the lectures. Accordingly, in tackling the exam, students do not need to make use of other reading materials, such as the GDPR Commentary edited by Kuner, Bygrave and Docksey—a text that not all students would have been able to access. However, students should not be penalized if they do utilize such materials.]

Please answer all questions. The questions do not have equal weight in the marking of the answers. Question 1 accounts for 40% of the final mark, question 2 for 10% of the final mark, question 3 for 10% of the final mark, question 4 for 10% of the final mark, and question 5 for 30% of the final mark. The word length for the entire answer is 3,000 words.

1. Brusque Business (BB) is a 'gig economy' company that, somewhat similar to Uber, operates a digital platform to connect car drivers with potential passengers in order to offer the latter cheaper and more efficient transportation than a traditional taxi service offers. BB has its head office in Frankfurt am Main and conducts its operations across Germany. As part of the 'Terms of Service' that are included in the agreement between BB and the drivers who use its platform there is provision for the payment of monthly 'bonus' amounts of money to drivers who meet

certain Key Performance Indicators (KPIs). The KPIs include criteria such as number of passenger rides per hour and customer satisfaction ratings. Calculation of the bonus payments is done by a computer program. Staff working in BB's payments department carry out sporadic checks of the computer calculations to make sure that the latter are roughly in line with the reported KPI measurements, and each bonus payment is accompanied by an email from BB's CEO, Mark Macho, to the driver concerned in the following terms: "Hi [name of driver]! You're doing really well and I have therefore decided that you deserve a bonus of [amount in Euros] for this past month's performance. Keep up the great service! Regards, Mark Macho". Do you think that the bonus payments system falls within the scope of Article 22 of the EU General Data Protection Regulation (GDPR), and if it does, what consequences does this entail for the ability of BB to keep the system operating? Provide reasons for your answer.

[**Answer:** There are two main lines of analysis called for here: (i) assessing the applicability of Article 22 GDPR to the bonus payments system (BPS); (ii) assessing the consequences of its possible application. A good answer must deal with both aspects. However, a good answer need not deal extensively with more general "threshold" issues, such as whether or not the BPS processes personal data or is subject to the requirements of the GDPR generally; it suffices to state that the BPS falls within the scope of the GDPR as it involves processing of personal data and does not benefit from the exemptions in Article 2 GDPR.

A good answer would then proceed to consider the basic requirements for Article 22 to apply, these being threefold: (1) a decision is made that is (2) based solely on automated processing or profiling, and (3) has legal effects or similarly significant consequences. In respect of the BPS, it is obvious that decisions are made; more contestable is whether the second- and third-listed requirements are met.

A good answer would note that the second-listed requirement entails absence of meaningful or genuine human involvement in the decisional process. In this respect, a good answer would reference the 2018 guidelines of the Article 29 Working Party (WP29)—endorsed by the European Data Protection Board (EDPB)—which elaborate that meaningful human involvement means oversight by "someone who has the authority and competence to change the decision" and who "considers all the relevant data". An excellent answer would also provide a brief explanation of the legal status of such guidance, stating, *inter alia*, that while WP29/EDPB guidelines are soft law and equivalent to "administrative practice" in the classical hierarchy of legal sources, they represent the considered views of experts in the field and are accorded considerable weight by judicial organs, noting, e.g., that they are often cited with tacit approval by the Advocates General of the CJEU. Hence, the guidelines may be considered as providing—at least as a point of departure—a fairly accurate indication of how the GDPR shall be interpreted *lex lata*. A good answer would then consider whether or not there is meaningful human involvement in the BPS. It ought to note that the email communication from BB's CEO—which pitches the bonus payment as his decision—is hardly decisive here, as he does not exercise any actual influence on the calculation and making of each individual payment (even if he has approved or initiated the BPS generally). As for the checks by the staff of BB's payments

department, these are described as “sporadic”, which suggests that human oversight is both irregular and rare and, concomitantly, insufficient to make the BPS a decision *support* system that falls outside the scope of Article 22(1). However, it is impossible to conclude definitely on this point without more facts on the frequency and intensity of the staff checks, and a good answer is not expected to reach a clear-cut conclusion here; what is important is that the answer lays out the various factors and discusses their weight, with some references to the WP29 guidelines.

Regarding the third-listed requirement, a good answer would observe that the BPS does not have obvious or direct legal effects but might have similarly significant effects. A good answer would go on to state that elaborating precisely the significant effects threshold is difficult—a difficulty also noted by the WP29—but that the inclusion of “similarly” indicates that the effects must have a degree of significance that roughly equates with legal effects and that this means, at the very least, that the effects must be non-trivial. A good answer might further reference the WP29 guidelines which state that the significant effects threshold may be met when the decision has the potential to “significantly affect the circumstances, behaviour or choices of the individuals concerned”, “have prolonged or permanent impact on the data subject” or “at its most extreme, lead to the exclusion or discrimination of individuals”. A good answer would then discuss whether the BPS has such qualities. Again, a good answer is not expected to reach a definite conclusion on this issue, but is expected to set out the various factors and consider their weight, in light of the WP29 guidelines. Some intrepid students might have managed to find a judgment handed down on 11 March 2021 by the Amsterdam District Court which held that an automated bonus payment system somewhat similar to the one in the case scenario did not have the requisite effect for Article 22(1) to apply, even though the court acknowledged that “obtaining a bonus will have a certain influence on the driver’s behaviour”. However, care should be taken in placing a great deal of weight on this judgment: it is a decision of a first instance court, and a factor behind its finding on this particular point was the complainant’s failure to adduce evidence that the system had the necessary effect. In the court’s view, data subjects have the onus of showing that a decisional system they dislike has the necessary effect on them, if they want to exercise their right under Article 22(1). For the purposes of the exam, there is no expectation that a student mention the evidentiary burden as this was not dealt with in lectures.

Moving to the second main line of analysis, this obviously proceeds on the assumption that the BPS falls within the scope of application of Article 22. Thus, it is somewhat independent of the conclusion a student might reach in respect of the first main line of analysis. So even if a student concludes that the BPS does not fall within the ambit of Article 22, it is expected that the student also considers the consequences were Article 22 to apply. A preliminary point that a good answer ought to deal with concerns the very nature of Article 22(1): is it a right to be exercised at the discretion of the data subject or a qualified prohibition on the decisional processes it covers? This issue has been dealt with fairly extensively in the lectures so a good answer would, at the very least, contrast the viewpoint of the WP29/EDPB (holding that Article 22(1) is a prohibition) with that of certain scholars, such as Luca Tosoni (holding that Article 22(1) is a right). An excellent (A) answer would argue that the latter viewpoint is probably most correct, and briefly cite Tosoni’s persuasive arguments in point. Due to the word count, though, there is no need for

a good answer to deal with this issue in detail. The most important point that a good answer must highlight here is that if Article 22(1) is a right, the BPS can operate without having to satisfy one of the criteria in Article 22(2)—in this case, contract or consent—so long as the system does not breach other requirements of the GDPR. If, however, Article 22(1) is a prohibition, the BPS may only operate if one of those Article 22(2) criteria is met. A good answer would go on to examine briefly the application of Article 22(2) in respect of each of the above alternatives. In respect of the former alternative (Article 22(1) as right), a driver would not be able to exercise their right (under Article 22(1)) if the BPS is contractually necessary (Article 22(2)(a)), whereas if Article 22(1) is a prohibition, BPS would only be able to operate if it is contractually necessary. So both alternatives lead to a consideration of whether the payment of bonuses satisfies the necessity criterion. This is an open question and, again, a good paper does not have to reach a definite conclusion here. However, it ought to note that a relevant factor will be the availability of other, less problematic means of achieving the goal of the BPS: as the WP29 guidelines state, "[i]f other effective and less intrusive means to achieve the same goal exist, then it would not be 'necessary'".

A good paper would further note that the consent criterion (Article 22(2)(c)) is probably not applicable because consent must be freely given and this prerequisite may be difficult to satisfy. The power relationship between BB and the drivers is very close to an employer-employee relationship (even if the drivers' formal legal status might be as self-employed contractors), and it is generally held that employees can only exercise free consent in very exceptional circumstances that involve no adverse consequences for them regardless of how they choose.

Finally, a good paper would turn briefly to the application of Article 22(3) rights. It would note that these rights mean that a driver will always be able to demand human review of the decisions generated by the BPS and also most likely demand *ex post* explanation of them. An excellent (A) answer would note in respect of the explanation right that this flows not just from the right to contest a decision in Article 22(3) but also from a range of other provisions in the GDPR, such as Articles 5(2), 13(2)(f), 14(2)(g) and 15(2)(h)).]

2. Consider the following variation on the scenario described in question 1. In order to help prevent instances of unruly, rude or violent passenger behaviour, BB decides that all drivers who use its platform must install a camera-like device in their cars. The device consists of a 5cm wide bulbous lens that is inserted into the foam layer on the ceiling of the car just above where passengers are usually seated. There is no sign posted in the car to alert passengers to the device, but the lens is clearly visible for passengers—and is meant to be so. However, the device does not have any function for recording or otherwise monitoring passenger behaviour—it is, in effect, a 'dummy' or 'fake' camera. After BB's decision is implemented, several passengers who take rides in cars with the devices installed react negatively to them. Believing that the instalment of the devices breaches the GDPR, the passengers request their local data protection authority to ban the use of the devices. Do you think that the instalment of the devices contravenes the GDPR? Provide reasons for your answer.

[**Answer:** This question can be dealt with very briefly. A good answer would conclude in the negative because the devices, while intrusive, do not collect or otherwise process personal data, and the GDPR only applies to processing of such data. A brilliant (A+) answer might note that this result arguably highlights a problematic gap in the GDPR's ability to safeguard privacy-related interests, but also note that some national laws, such as Norway's Personal Data Act (see § 31), provide protections against such devices.]

3. Consider the following variation on the scenario described in question 1. An Indian company, Remote Control (RC), which has its head office in Mumbai, acquires 60 percent of BB's shares and thereby takes control over BB. RC decides to continue BB's driver service operations in Germany, using the platform developed by BB and retaining BB's staff. Do you think that RC is now subject to the requirements of the GDPR by virtue of Article 3(1) GDPR? Give reasons for your answer.

[Answer: This question is tricky due to three factors. First, the scenario involving RC does not provide sufficient facts to determine precisely the nature of RC's relationship with BB, and the nature of this relationship is important for determining how Article 3(1) GDPR applies. Secondly, the wording of Article 3(1) is far from easy to understand. Thirdly, the question implies, incorrectly, that Article 3(1) is about "capturing" particular entities such that they need to abide by the GDPR: rather, Article 3 identifies instances of processing that are caught by the GDPR, not entities that are caught by the GDPR. A good answer should highlight at least the first-mentioned factor. Thus, a good answer is not expected to provide a conclusive answer in the positive or negative; more important is the reasoning it sets out. Nonetheless, a good answer ought to conclude that RC is *possibly* or even *probably*—but *not necessarily*—caught by Article 3(1) in the context of the relevant processing.

Going into more detail, it is fairly clear that, by acquiring a controlling stake in BB and deciding to maintain BB's data-processing operations, RC has become a controller. Less clear is the extent of that control over data-processing operations: has RC taken over to such a degree that BB has become a mere processor or is BB now a joint controller (with RC)? The latter possibility assumes, of course, that a subsidiary can co-determine purposes and means together with a holding/parent company. Such an assumption is not unrealistic, but, again, there are insufficient case facts to determine whether it is true for this particular relationship.

It is also clear that the processing takes place in the context of the activities of an establishment of a controller or processor in the EU. BB is definitely established in the EU, but one cannot conclude whether its establishment is as joint controller or as processor. Less clear is whether RC now has an establishment in the EU. Here a good answer would cite recital 22 GDPR which states: "Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary

with a legal personality, is not the determining factor in that respect." Hence, the key criterion is whether RC engages in "effective and real exercise of activity through stable arrangements", regardless of the legal formalia. A good answer will likely argue that RC is possibly if not probably so engaged but that one cannot be certain due to the paucity of details of the actual (as opposed to legal) relationship between BB and RC. An excellent (A) answer would additionally note that the mere fact that a controller uses a processor that is established in an EU member state does not mean that the controller is also established in that state (a point also made by the EDPB in its guidelines 3/2018 on territorial scope).]

4. In the context of measures to combat the ongoing COVID-19 pandemic, the respective data protection authorities of the Scandinavian countries have stated that information that someone is in quarantine is not "data concerning health" in the meaning of Article 4(15) GDPR when there is no further information provided on the cause of quarantine. The same applies in respect of information that someone has been in or returned from a "risk area" (i.e. an area where there is a relatively high degree of virus transmission). Do you think the authorities' viewpoint is correct? Give reasons for your answer.

[**Answer:** This question can be dealt with very briefly. A good answer would conclude in the negative because: (i) the notion of "data concerning health" shall be construed broadly (an excellent answer might include a reference here to the CJEU judgment in *Lindqvist*); (ii) recital 35 GDPR specifically mentions information on "disease risk" as falling within the health data category; (iii) quarantine measures are usually linked to a *risk* of contamination, and no further information is generally necessary to make that connection; and (iv) that connection brings with it a potential for stigma and unfair discrimination—a potential that the GDPR is intended to counter through adopting a broad definition of health data and subjecting such data to extra stringent protections.]

5. Consider the following claim: "The Court of Justice of the European Union has expanded the definition of 'controller' in the GDPR to such a degree that the definition has lost connection with the core concept of control". Discuss the validity of the claim in light of the Court's jurisprudence on joint controllership, focusing on its rulings in Cases C-210/16, C-25/17 and C-40/17.

[**Answer:** This is a relatively difficult task as it demands a good understanding of fairly complex case law that has recently evolved around the notion of joint controllership and that may well undergo further refinement in light of the controversy it has created. The task also places relatively high demands on students' ability to structure their discussions in a concise, clear and cogent way, and to engage in *lex ferenda* type reflection. That said, *lex ferenda* elements are baked into numerous parts of the course, so this sort of task will not take students by surprise.

Moreover, the lectures have dealt with the notions of controller and joint controllership in considerable detail, although they have not parsed the relevant case law in great depth. All up, though, examiners ought to adopt a generous and somewhat forgiving attitude when assessing the answers here, also in light of the factors mentioned at the beginning of the guidance notes. Further, good answers may adopt quite different ways of structuring and presenting their discussions, so what follows should not be regarded as necessarily the optimal template.

A good answer would briefly describe both the concept of control that is central to the definition of "controller" in Article 4(7) GDPR and the concept of joint control, as elaborated in the three CJEU judgments that are the focal points of the claim in question (i.e. *Wirtschaftsakademie*, *Jehovan todistajat* and *Fashion ID*). A good answer ought to highlight at least the following two important points. First, the notion of control hinges on actual exercise of influence over the purposes and means of processing and does not necessitate access to or processing of the data. Secondly, joint controllers do not necessarily share equal responsibility for all "stages" or facets of the data-processing activities in which they are engaged; instead, responsibility of each joint controller will vary from one stage to another, according to the degree to which they exercise control in the particular context. A brilliant (A+) answer might also note that the CJEU is rather inconsistent in its terminology, sometimes using the terms "liability" and "responsibility" interchangeably, despite these terms usually denoting different legal consequences.

A good answer should then turn to the claim in question and probe its validity. In support of the claim is the fact that the CJEU has made it relatively easy for an entity to be cast in the role of joint controller in situations where the entity plays a fairly modest if not marginal role in a data-processing system. This is exemplified especially well by the outcome in *Fashion ID* where the mere insertion of a Facebook plug-in was sufficient to make Fashion ID a joint controller with Facebook, despite the latter having most power over the data-processing system. This development risks softening the distinction between controllers and processors, and, concomitantly, risks diluting the essence of control. However, a good answer would also note that other aspects of CJEU jurisprudence undermine the claim's validity. In particular, the Court's insistence that the GDPR's obligations for controllers are commensurate with those stages in which they actually exercise control goes against the grain of the claim and shows that the Court is, at the very least, concerned to ensure "a reasonable correlation between power, control, and responsibility" (to use the words of Advocate General Bobek in *Fashion ID*).]