JUS5630: Exam 2023 – Assessment Guidance Notes

[**Overall remarks:** The exam is fairly straightforward, particularly as it is an open-book exam. However, it is also very challenging because students have had to write their answers in a tight time frame and sitting in an examination room with numerous other students. Adding to the challenge is that many of the students will be unfamiliar with this sort of exam setting. During the last few years, home exams lasting 24 hours have been the norm, and such exams are considerably more relaxing. So many students will likely have struggled with nervousness and paucity of time to a greater degree than before. These factors ought to be taken account of when grading their answers.

Given the four-hour time limit, students cannot be expected to analyse in detail all possibly relevant rules, perspectives or arguments. Hence, students' treatment of these will necessarily be relatively superficial. This applies also to papers that would qualify for a top grade. Further, students were informed prior to the exam that they ought to be concise in their answers and that they may even resort to bullet-points if necessary. Accordingly, brevity or use of bullet-points should not be penalized.

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 they include a bibliography at the end of their exam paper. Moreover, they are expected to be able to answer the exam questions on the basis of the reading materials listed as pensum, lecture handouts, and case law referenced in the lectures (particularly cases listed in the 'must read' set of cases, as flagged below). Thus, 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. However, students should not be penalized if they do utilize such materials.]

Please address the following exam tasks, applying European law on privacy and data protection.

In grading the answer, the exam tasks will be weighted as follows. The answer to exam tasks 1(a), 1(c) and 2 will count for approximately 75% of the final grade (each answer counting approximately 25%), while the answer to task 1(b) will count for approximately 10% and the answer to task 3 approximately 15%.

1. Consider the following scenario: Alexandra (A), a 25 year old student living in Oslo, applies for a credit card issued by Big Business (BB). Her application is granted. The credit limit for A is initially set at NOK 40,000 [NOK = Norwegian kroner]. This is the standard default limit that BB sets for people above 20 years of age living in Norway. Six months later, BB reduces the limit to NOK 25,000. The reduction is not based on an individual assessment of A's repayment history; indeed, A has not had any documented problems in repaying amounts owing through use of the credit card. The reduction is based on computer assessment of statistical demographic factors of the area in which A lives—an area where numerous low-income earners and recipients of social welfare benefits reside. Alexandra thinks that the reduction is unfair. Having studied data protection law, she is aware of Article 22 of the GDPR. She complains to BB alleging that Article 22 has been breached. BB responds by

claiming that there has been no breach of Article 22 as the data that is the basis for the reduction is not personal data, only aggregate statistical data. A then brings a complaint to the Norwegian Data Inspectorate (Datatilsynet), alleging breach of Article 22.

1(a) You are the case officer at the Data Inspectorate charged with assessing the merits of the complaint and BB's response. Provide your assessment of both and give reasons for your viewpoints. Your answer need only focus on Articles 22 and 4 of the GDPR.

[Answer: As indicated, this task tests students' knowledge of Articles 22 and 4 GDPR, along with their interaction. Thus, a good answer must consider the application of both sets of provisions. A good answer will first highlight why and how these two sets of provisions are potentially engaged in relation to the case scenario. Article 22 is potentially engaged because there appears to be a decision of the kind described in Article 22(1). Article 4(1) is potentially engaged because of BB's claim about the nature of the aggregate statistical data, and Article 4(4) is potentially engaged because the reduction in credit limit might be based on profiling. At the same time, a good answer also needs to discuss whether and how the provisions of Article 4(1) and (4) are legally relevant for resolving the application of Article 22.

Regarding application of Article 22, a good answer would note the four preliminary conditions for such application: (1) a decision is made; (2) the decision is based solely on automated processing; (3) the decision has legal effects or similarly significant consequences; and (4) the decision involves automated processing, including profiling. A very good answer would also briefly discuss the basic nature of Article 22(1)—is it a qualified prohibition or a right?—and the effects of this characterisation for the outcome of the dispute. In relation to the latter issue, a very good answer would note that the prohibition line so far finds most favour with DPAs (*viz.* EDPB Guidelines of 6 February 2018, p. 19) and has also been followed by Advocate General Pikamäe in Case C-634/21, *Schufa Holding*, para. 31, but that a cogent and convincing case can be made for the opposite viewpoint (viz. the article by Tosoni, referenced in lectures). It is not necessary that students reach a final conclusion on the issue; the important point is that they flag it and briefly outline the opposing arguments. They should also discuss whether the issue has any real bearing on the outcome of the dispute; it probably does not, although the line that Article 22(1) is a qualified prohibition perhaps makes it easier for A to argue that the provision has been breached. The strength of that argument, however, would depend on whether any of the exceptions/qualifications in the other three paragraphs of Article 22 have been met—and a good answer would have to canvass that question regardless.

Regarding that question, a good answer would indicate that A has not consented to the reduction of her credit limit, nor is the reduction provided for by law. BB might be able to argue that the reduction is necessary for the performance of the contract with A, but the argument is weak especially given that necessity is to be construed strictly. Thus, a good answer would conclude that the qualifications to the prohibition or right in Article 22(1) are most likely not met.

This means that the dispute will turn on whether the four conditions for applying Article 22(1) are fulfilled. A good answer would indicate that the key conditions here would be the first, third and fourth from the list above—i.e. whether a decision is made, whether the decision has legal effects or similarly significant consequences, and whether the decision involves automated processing, including profiling. In respect of whether a decision is made, a good answer would note that the term 'decision' ought to be construed broadly given its use in a

fundamental rights context, and that it connotes the taking of a position or making of a choice of binding character—as pointed out in the lectures and also in AG Pikamäe's opinion in *Schufa Holding* (paras. 37-38)—which is the case here. As for the consequences of the decision, these are most likely to be regarded as sufficiently significant: A's credit limit has been almost cut in half and this could detrimentally impinge on her ability to purchase important goods or services (see also the aforementioned EDPB Guidelines, p. 22, although students should not be penalised for not referencing these as this aspect of them was not highlighted in lectures).

As for the final condition (i.e. that the reduction in credit limit is based on automated processing, including profiling), a good answer would note that it is in this context that BB's claim that Article 22 is not applicable becomes legally relevant. In respect of that claim, a good answer would point out the following:

- The definition of profiling in Article 4(4) is such that profiling must involve processing of personal data, but the personal data need not relate to the person seeking to invoke Article 22(1) (as also pointed out in the aforementioned EDPB Guidelines, p. 22)—thus, the data used to reduce A's credit limit do not have to be personal data regarding A.
- However, Article 22(1) is formulated such that profiling is not a necessary condition for its application (the word 'including' is best understood as indicating that profiling is an alternative condition; see also the aforementioned EDPB Guidelines, p. 8, highlighted in the lectures). Thus, Article 22(1) may apply without profiling taking place, as long as there is otherwise 'automated processing' behind the decision (and the other conditions for applying Article 22(1) are met).
- Automated processing as it is set out in Article 22(1) does not need to involve processing of personal data; what is decisive is the automation element, which is clearly present in the present scenario. Thus, BB's claim is ultimately irrelevant for the application of Article 22(1).

Finally, a good answer would also consider the merits of BB's claim that aggregate statistical data is not personal data, but consideration need only be cursory. In this context, a good answer would note that aggregate statistical data would ordinarily not qualify as personal data as they do not permit the necessary level of individuation that is built into the definition of personal data in Article 4(1), but that the definition is broadly construed (*viz.* the CJEU's judgment in *Nowak*) and that, with big data analytics, it is increasingly possible to link aggregate data to particular individuals, and, if such linkage is possible through reasonably likely means (*viz.* recital 26 GDPR) then the data used by BB to reduce A's credit limit may qualify as personal data.]

1(b) Consider the following variation on the above scenario: A threatens BB that she will go to court to sue BB for breach of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). You are a lawyer employed by BB to provide legal advice on the merits of her threat. Provide your advice to BB and give reasons for your advice. Your answer need only focus on the ECHR.

[Answer: This tests students' knowledge of the procedural basis for bringing claims of ECHR violation to a court. The basic point that a good answer should make is that A cannot sue BB in court for BB's alleged breach of Article 8 ECHR as Article 8 speaks primarily to the obligations of states parties to the Convention (i.e. the obligations of Norway). In this regard, Article 8 is only indirectly relevant for private actors such as BB even though such actors must respect the rights laid out in ECHR as they are also rights inherent in Norwegian law. Accordingly, A's dispute with BB, in this context, would have to be formulated as a claim that Norway has breached its obligations under Article 8 ECHR by not ensuring, through its own laws, that BB's actions respect A's right(s) under Article 8. A good answer would conclude that A's threat as it currently stands has little chance of success.]

1(c) Consider the following subsequent scenario: A inherits a substantial amount of money and decides that now is the right time to buy an apartment in Oslo, particularly due to the flattening out of real estate prices. In light of her poor experience with BB, she approaches another bank, Easy Loans (EL), to set up a meeting regarding a possible bank loan for the apartment. She contacts EL via e-mail to set up the meeting. At the meeting, A does not get a good impression of EL and she decides not to become a customer of the bank. EL, however, plans to add A's e-mail address, <alex@greenparty.org> to its customer e-mail database and then allow Meta/Facebook to match that database with the list of e-mail addresses held by Meta/Facebook, in order to target the individuals concerned with online advertising of EL's full range of financial services.

You are the Data Protection Officer of EL and asked to provide advice as to whether EL's plan conforms with EL's obligations under the GDPR. Provide your advice and give reasons for your advice, including references to the relevant provisions of the GDPR in light of case law from the EU Court of Justice and guidance from the European Data Protection Board. You do not need to assess the legal position of Meta/Facebook.

[Answer: This task primarily tests students' knowledge of Articles 4(1), 4(7), 5, 6 and 9 GDPR. A good answer would note why these provisions are relevant and how they play out in relation to EL's plans. Of these provisions, Articles 4(1) and 4(7) can be dealt with relatively briefly; a good answer would focus mainly on Articles 5, 6 and 9. Nonetheless, a good answer would initially have to address the status of EL as possible controller. On this matter, it is fairly clear that A is a controller in respect of the first envisaged use of A's email address (i.e. adding the address to the database) and is then a joint or co-controller in respect of the matching and targeting processes. Here reference would be made to the CJEU judgments in *Wirtschaftsakademie* and *Fashion ID* (both on the 'must read' list of cases). Reference might also be made to the EDPB Guidelines 08/2020 (pp. 11ff) although students should not be penalised for not referencing these guidelines as they were not flagged in the lectures.

As for the issue of whether A's email address qualifies as personal data under Article 4(1), again, the conclusion can be quickly drawn that it is personal data, with references made particularly to the CJEU judgments in *Breyer* and *Nowak* (both also on the 'must read' case list).

A good answer would then address the status of the email address as one of the categories of data listed in Article 9(1). Given that the email address appears to flag A's political opinion or, less directly, philosophical beliefs, it would seem to fall within the class of data protected by the prohibition in Article 9(1). A good answer would approach this matter in light of the CJEU judgment in Case C-184/20, *OT*, paras. 117ff (on the list of 'must read' cases) which

takes a broad view of when personal data may be regarded as sensitive for Article 9 purposes—i.e. data from which one of the data categories in Article 9(1) can be *indirectly* inferred, may be protected by Article 9. If, as is most probable, the email address is sensitive pursuant to Article 9(1), a good answer would then consider whether its envisaged use by EL would be permitted under Article 9(2) as a derogation from the Article 9(1) prohibition on processing. The obvious conclusion to be drawn would be that none of the Article 9(2) bases for processing apply in this case.

Even though Article 9 most likely prevents EL's envisaged uses of A's email address, a good answer would briefly consider the application of Articles 5 and 6. Article 5 is engaged because EL's plans involve a re-purposing of personal data that would be in breach of the compatibility criterion of the purpose limitation principle in Article 5(1)(b), as elaborated in Article 6(4). On this point, a good answer would flag as particularly relevant that EL's envisaged use of the email address would be beyond A's reasonable expectations (*viz.* recital 50) and otherwise be insufficiently close, logically, to the initial purpose for registering the address. On these points, a good answer *might* refer to the CJEU judgment in Case C-77/21, *Digi TávközlésiésSzolgáltatóKft. v NemzetiAdatvédelmiésInformációszabadságHatóságon* (paras. 36-37) but would not have to as the judgment is not on the list of 'must read' cases nor was it dealt with at length in lectures.

Finally, regarding other provisions of Article 6, a good answer would briefly canvass whether contract (Article 6(1)(b)) and legitimate interest (Article 6(1)(f)) may qualify as a suitable lawful basis for the envisaged use of the email address. A good answer would conclude that neither of these bases is applicable in this case, particularly due to the necessity criterion embedded in both. Further, it is unlikely that the planned uses of the email address can be considered 'legitimate' as they do not accord with A's reasonable expectations (see also the aforementioned EDPB Guidelines, p. 20]

2. Consider the following statement: "The provisions of Article 25 GDPR are a welcome innovation in EU data protection law". Do you agree? Give reasons for your view.

[**Answer:** This task tests students' ability to reflect over the pros and cons of Article 25 GDPR. A good answer would first briefly outline the content of Article 25 and what it aims to achieve. Thereafter, a good answer would note that Article 25 is certainly an innovation as there was no proper equivalent of it in the Data Protection Directive (95/46/EC). A good answer would then discuss the degree to which that innovation is *positive* ('welcome'). One possible problem of Article 25 is its diffuse and complex formulation which leads to interpretative difficulties—difficulties that are exacerbated for the engineering community to which Article 25 is supposed to speak, indirectly if not directly. Another possible problem is related to its utility. In this regard, a very good answer might note the claim by Waldman that Article 25 is not just difficult to comprehend but ultimately superfluous. Yet another possible problem is that Article 25 might stymie innovation by reducing the freedom of developers of information systems to generate novel products or services. On the other side, a good answer would note that the aforementioned problems may be viewed as less real than they first appear. For example, there is now relatively detailed guidance on the meaning and operationalization of the provisions of Article 25 (*viz.* the EDPB Guidelines 4/2019 which have been referenced in lectures). Further, building on the EDPB's Guidelines and Bygrave's work (flagged in lectures), it could be argued that Article 25 is not superfluous but has both pedagogical and 'cementing' functions: it spells out what is necessary to ensure that the GDPR is properly embedded or cemented into information systems development. In respect

of innovation, the point could be made that Article 25 contributes to ensuring that innovation is societally 'responsible'; moreover, its provisions are pitched at such a high level of generality that they do not necessarily steer innovation in an overly restrictive manner.

The aforementioned pros and cons are just examples of what a good answer might mention; they are not exhaustive. Bygrave's paper on Article 25 in *Oslo Law Review*—which is required reading—sets out additional problematic aspects of the provisions]

3. A Chilean company, Great Shoes (GS), with headquarters in Santiago runs a business selling shoes to customers in Chile and neighbouring countries in South America. It engages a Spanish company, Fast Computing (FC), established in Barcelona, to process personal data relating to GS's customers. GS's business operations are directed only at the South American market and its customers are all in South America.

You are a lawyer employed by FC and you are asked to determine whether the GDPR applies to GS and to FC's processing of GS's customer data. You are also asked to determine which provisions of the GDPR may apply to FC's processing of GS's customer data, if the processing falls within the GDPR's ambit. Provide reasons for your answer.

[**Answer:** This task primarily tests students' knowledge of Article 3 GDPR. It secondarily tests their knowledge of GDPR provisions that are relevant for processors (and not just controllers). A good answer would first note that the GDPR will only be applicable if the customer data qualify as personal data, pursuant to the definition in Article 4(1) GDPR. The scenario indicates that the relevant customer data are, indeed, personal, so there is no need for a good answer to provide an in-depth analysis of what is personal data in this context. The next important point that a good answer ought to make is to identify Article 3 GDPR as laying down the principal rules for when the GDPR applies to the processing of personal data, particularly processing with a cross-national dimension, and that these rules cover several alternative situations, differentiated according to where controllers or processors are established and the context of the processing. A good answer would go on to note that, applying the definitions of 'controller' and 'processor' in Articles 4(7) and 4(8) GPDR, GS qualifies as the controller of the customer data while FC qualifies as the processor. A good answer would thereafter note that GS is not 'established' in an EU/EEA member state for the purposes of Article 3(1) GDPR, nor does it seem to engage in any of the activities covered by Article 3(2) GDPR—it only targets South American customers and there is no indication that it monitors data subject behaviour within the EU/EEA. Thus, the conclusion would be that GS's operations fall outside the scope of the GDPR.

As for FC, a good answer would note that it is established in an EU member state (Spain) and its processing occurs in the context of its activities as an entity established in the EU. Hence, the conclusion would be that FC's operations fall within the scope of the GDPR. A good answer would finally determine which of the GDPR's provisions apply to FC's processing operations. The list would include Article 28(2), (3), (4), (5) and (6), Article 29, Article 30(2), Article 31, Article 32, Article 33, Articles 37 and 38, and the provisions in Chapter V dealing with transfers of personal data to third countries and international organisations.]