Privacy and Data Protection (JUR 1630)

Spring 2022

Exam question: guidance notes

[**Overall remarks:** On its face, this exam is quite straightforward. It is intended to encourage students to reflect upon the lawfulness of the planned data-processing system against a potentially large range of provisions of the GDPR. It also gives students a fair amount of discretion as to which of these provisions they want to focus upon in their assessment. At the same time, however, the open-endedness of the exam is quite challenging as it gives students relatively little guidance for structuring their answers and it tests the degree to which they have a comprehensive understanding of the GDPR as a whole, rather than just particular provisions.

Students were only permitted to write an answer with a maximum of 2,000 words, and this means that they cannot canvass in detail all possibly relevant provisions. Hence, students' treatment of the provisions (or at least some of them) will necessarily be superficial, with little room for discussion. Students were also informed prior to the exam that they ought to be very 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 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. 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.]

Exam question

Perfect Features (PF) is a company specialising in biometrics applications. It has developed a facial recognition system that can be deployed in pubs, bars, restaurants and similar sorts of venues to assist in ensuring that persons who enter these venues have been vaccinated against Covid-19. Instead of people themselves having to present proof that they are vaccinated at the venues' entrances, their faces are scanned and matched against a central database containing information on their vaccination status. Great Dining (GD) is a company that owns and operates a chain of pubs and restaurants in Sweden and Norway. It would like to use PF's system in its

pubs and restaurants, and, to that end, have the system linked up to the vaccination databases maintained by the health authorities in Sweden and Norway.

Is GD's planned use of PF's system permitted pursuant to Regulation 2016/679? And is there any further information that you would need before being able to determine the lawfulness of GD's plans? Give reasons for your answer.

[**Answer:** First, note should be made of the exam parameters. The exam requires focusing primarily on the lawfulness of GD's activities, not those of PF. However, students should keep in mind that there may be aspects of PF's system that impact the lawfulness of GD's activities. Further, the lawfulness of those activities is to be assessed pursuant to the GDPR only; there is no need to consider other laws, such as sectoral national laws of Norway or Sweden on biometrics or health databases. However, a very good answer would note that the GDPR is to be interpreted in light of the EU Charter of Fundamental Rights and, less directly, the European Convention for the Protection of Human Rights and Fundamental Freedoms, and that linkage to the vaccination databases of the two countries would be governed by sectoral national legislation. A student is not required to show knowledge of the details of such legislation; rather, those details could be identified as part of the "further information" that is relevant for determining the lawfulness of GD's plans.

A good answer would state at the outset that GD's planned use of the biometrics system would seem to involve processing of personal data (see Arts. 4(1) and 4(2) GDPR), that these data are also both biometric and health data (see Arts. 4(14) and 4(15) GDPR), and that GD's status under the GDPR is that of controller (see Art. 4(7) GDPR). A very good answer would elaborate on the definition of biometric data (see Art. 4(14)), emphasising that it covers both *identification* and *verification/authentication* functionalities, and that GD's planned use of PF's system seems primarily to involve identification because it relies on matching facial data against a centralized database (i.e. a 1:n comparison as opposed to a 1:1 comparison).

A good answer would then state that the lawfulness of GD's planned use of the system will depend on it being able to meet a large number of requirements under the GDPR. Primary requirements are that the system's processing of personal data conforms to the core principles set out in Art. 5, which means, *inter alia*, that processing is for specified, explicit and legitimate purposes (see Art. 5(1)(b)), transparent and fair (see Art. 5(1)(a)), and governed by appropriate technical and organisational measures to ensure the security of the personal data involved (see Art. 5(1)(f); see too Arts. 32 and 25). Another primary requirement is that the processing has a lawful basis under Arts. 6 and 9. A good answer would observe that whereas Art. 6 applies regardless of whether the processing is for purposes of identification or verification, Art. 9 applies when biometric data are used 'for the purpose of uniquely identifying a natural person' (Art. 9(1)), which is the case here. Thus, a good answer would go on to state that GD's planned scheme is prohibited under Art. 9(1) unless it falls under one of the exceptions listed in Art. 9(2). There are three possibly pertinent exceptions: explicit consent (Art. 9(2)(a)), substantial public interest (Art. 9(2)(g)) and public health (Art. 9(2)(i)). A good answer would note that all of these

exceptions must be interpreted stringently in light of the sensitivity of the data involved and the normative importance of the rights and freedoms at stake (these being anchored in the Charter and ECHR), and that, concomitantly, it will be difficult to show that they are apply to GD's planned system.

Regarding consent, in addition to being explicit, it must also satisfy the other requirements of valid consent (namely, that it be freely given, specific, informed, unambiguous and manifest in a clear affirmative action: Art. 4(11)), all of which may pose significant challenges. Further, the data subjects would have to be informed of the possibility of withdrawing their consent (see Art. 13(2)(c)). On the face of the scenario, there is no mention of consent, but arguably some sort of carefully calibrated consent mechanism could operate within the envisaged framework and might be able to meet the requirements of the GDPR.

Regarding the exceptions for substantial public interest (Art. 9(2)(g)) and public health (Art. 9(2)(i)), both of these are pertinent inasmuch as GD's planned scheme is motivated by the need to contain the public health threat of the Covid-19 pandemic. And a very good answer might point to recital 52 which mentions "prevention or control of communicable diseases and other serious threats to health" as amongst the interests protected by the derogation from the prohibition in Art. 9(1). However, a good answer would also note that both exceptions require legislative authority, and in the case of the public health exception, such authority must additionally set out appropriate safeguards. Moreover, both exceptions are subject to stringent requirements of necessity and proportionality. After elaborating briefly on these requirements (ideally with references to relevant CJEU case law, such as Case C-524/06, *Huber* or Case C-13/16, *Rīgas satiksme*), a good answer would find that GD's planned scheme is unlikely to meet them. This is largely because it is doubtful that the goal in question (i.e. ensuring that persons who enter the venues have been vaccinated) cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of the data subjects.

Thus, all up, a good answer would conclude that the scheme is probably not lawful under the GDPR, primarily due to the operation of Art. 9. A good answer would also make clear that the scheme might fall foul of a number of other GDPR requirements as well. For example, to the extent that the scheme would involve a fully automated decision with legal or similarly significant effects for the data subjects, suitable measures would need to be in place to provide the latter with meaningful information about the decisional logic (see Art. 13(2)(f)) or to demand such information (see Art. 15(1)(h)), and to permit data subjects to contest the decision or demand human intervention (see Art. 22(3)). Other examples include the requirements of data protection by design and by default (Art. 25) and security (Art. 32).

As for the question regarding further information that might be necessary to determine the lawfulness of GD's plans, a good answer would respond in the affirmative, noting that more detail is needed on what sort of consent mechanisms would be operating (for the purposes of Art. 9(2)(a)). A good answer would also state that numerous other details would be necessary in order to assess accurately the scheme's lawfulness against a large range of other GDPR requirements, such as those in Arts 5, 12, 13, 22, 25 and 32. Further information would also be

desirable regarding the legislative frameworks for using and linking up to the vaccination databases of the Norwegian and Swedish health authorities.

Finally, an excellent answer *might* observe that the scenario assumes the existence of a centralized database containing the "master template" of the facial characteristics but omits details about the organisational framework for such a database. The database on vaccination status could, in theory, contain such a template but the health authorities in Norway and Sweden are unlikely to have registered the facial characteristics of those who have been vaccinated. So the scenario assumes that there is another database with those characteristics. In theory, PF could be operationally responsible for this database, or it could be operated by another private sector actor. However, we do not know "the facts" here. And obviously these missing facts will be crucial for any holistic assessment of the lawfulness of the scheme. However, failure to highlight this point should not detract from a student's grade as JUR1630 does not aim to impart detailed knowledge of the mechanics of biometric systems (hence, the use of "*might*" in the first sentence of this paragraph).]