JUS5630 H22 Marking Guidance
Peter Davis

Overall remarks: Students were only permitted to write an answer with a maximum of 3,000 (+10%) words, and this means that they cannot canvass in detail all possible issues or arguments in the questions. Hence, students' treatment of the provisions and arguments (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 (the advantage of doing so is that a bibliography is not included in word count). 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 penalised if they do utilise such materials.

Answer the following two questions. Expressed as percentages of the final grade, the answer to question 1 will count for approximately 70% of the final grade. Question 2 will count for approximately 30% of the final grade. Please note that Question 2 is related to the facts in Question 1.

Question 1 (70%)

PuntClub (**PC**) is an online gambling company that operates solely in the EU. It offers various gambling products, including sports betting and casino-style games like blackjack and roulette. Most of its profits come from a small portion of users that are frequent users of the site, who might be described as 'problem gamblers'.

Recently, PuntClub has noticed a downturn in its profitability. It has attributed this downturn to various governmental initiatives (at the EU and Member State level) that have sought to reduce the impact of problem gambling. These initiatives include the roll-out of counselling services directed at problem gamblers, and laws requiring that gambling companies (including PuntClub) allow individuals to 'self-exclude' from using their services for a period of 6 months.

In an attempt to increase profitability, PuntClub decides to implement an aggressive, data-driven marketing strategy. It internally develops a marketing tool called 'Discrimin8' (**D**) that uses big data analytics and artificial intelligence to optimally target its users with advertisements and promotions. Discrimin8 relies on a large quantity of information to function effectively, including data derived from its users (e.g. users' age, gender, address,

gambling habits, gambling gains or losses, and types of games and sports bet on) and data from other sources (e.g. statistics, publicly available information, information about the win rates of its games, and sport schedules and results). Discrimin8 automatically (i.e. without human intervention) delivers different advertisements and promotions to its users at different times and frequencies with the goal to maximise PuntClub's profits.

When users sign up to PuntClub online, they encounter a checkbox that reads as follows:

'☐ *I agree with the **terms and conditions** and the **privacy policy***'

Users must click on the checkbox if they wish to create an account with PuntClub that enables them to gamble on the site. The text '**terms and conditions**' and '**privacy policy**' contain hyperlinks to longer PDF documents.

Within the privacy policy PDF document is a heading 'Purposes', which contains the following text:

'We may use your personal data to provide service functionality, comply with our legal requirements, and enhance user experience. This includes processing your data for:

- *Registering and verifying your account*
- *Analysing use of our site and apps*
- *In-app or in-service personalisation*
- *Marketing*
- *Complying with anti-money laundering laws*
- *Sharing with our trusted third parties...'*

Brad (**B**) is a self-described gambling addict who has recently taken steps to address his addiction. His preferred gambling website was always PuntClub, but 5 months ago he put himself on the 'self-exclusion' list, so he is currently unable to access their services.

Recently, Brad noticed he was receiving a large amount of promotional material from PuntClub through his email and when browsing the web through advertisements. Brad feels that PuntClub or its algorithms 'know' that he is a problem gambler who is only 1 month away from being able to access his PuntClub account when the 6 month 'self-exclusion' period expires. Brad would like to know what data PuntClub has about him and why PuntClub seems to be targeting him with advertisements. He would also like this perceived targeting to stop.

Advise Brad on his rights under the GDPR to this end, and how he can exercise those rights, with respect to PuntClub's processing of his personal data.

The scenario is adapted from a report by Cracked Labs entitled 'Digital Profiling in the Online Gambling Industry' (that students are not expected to be aware of). The scenario is relatively lengthy, whilst simultaneously not always providing sufficient detail for students to reach firm conclusions. Therefore, it is to be emphasised that the following is guidance only; with students able to come to different conclusions from the available facts if reasonable to do so and properly supported. By way of example, it might reasonably be

argued that (certain of) B's personal data is a sensitive category of personal data under Article 9 GDPR, so far as his gambling 'addiction' might be a diagnosable mental illness – especially given the CJEU's apparent expansive approach to Article 9 evinced in Case C-184/20 *OT v Vyriausioji*. Nonetheless, the below proceeds on the basis that the data processed is 'ordinary' personal data.

The question is fairly difficult, and there are some particular challenges that students must face given the format and question, e.g.:

- identifying the key issues and areas of controversy to spend time/words on, given the lengthy facts and limited guidance on what issues are to be tackled;
- relatedly, being concise given the restrictive word limit; and
- being careful to tailor the response to the ultimate question asked - which is directed towards advising B, the data subject, rather than PC, the controller.

Students that give cogent, practical advice to B on his rights and how best to exercise them should be rewarded for doing so.

As a point of departure, it is fairly uncontroversial that the GDPR applies in this case, with PC as controller and B as a data subject. Data subjects enjoy an extensive menu through which they may exercise their rights under the GDPR, including through the controller directly, through their national DPA (Article 77(1) GDPR), and through national courts. A good answer would mention at least the former two (i.e. controller and DPA). It is not necessary to dwell significantly on judicial remedies in GDPR Chapter 8, since much depends on national law, but a *very good* to *excellent* response may at least give passing mention to this avenue, if not provide more detail.

The text of the question highlights three items that B wishes to address:

- what data PC has about him;
- why PC seems to be targeting him with advertisements; and
- making the perceived targeting stop.

As worded, however, the question is able to be interpreted more broadly to include other possible available courses of action for B (e.g. an action for compensation under Article 82(1).) However, a *good* answer would at least address these three items.

As for the first item, a *good* answer would note access rights under Article 15 GDPR that can be directly exercised by B against the controller. A *very good* answer may also note that, under Article 15(1)(h), B also has the right to know about information about 'meaningful information about the logic involved' of 'automated decision-making', which would also cover the second item.

Elaborating on the second item, In addition to access rights under Article 15, a *good* answer would also note the possible application of Article 22 GDPR. A *very good* answer would ponder whether this provision applies, given it only operates where a 'decision based solely on automated processing, including profiling produces legal effects concerning him or her or similarly significantly affects him or her'. An *excellent* answer might refer to the 'A29WP Guidelines on Automated individual decision-making and Profiling for the purposes of

Regulation 2016/679' endorsed by the EDPB, and pontificate over whether decisions made by D about B come within the scope of Article 22.

So far that an answer concludes that Article 22(1) is likely applicable, a *very good* answer would, in this vein, point to the possible right to an explanation of an automated decision, as indicated in recital 71. An *excellent* answer might question whether such a right exists, given its lack of explicit recognition in the operative provision, and pointing to academic debate on point. Overall, a *very good* answer would provide some insight into what precisely B may be able to find about P's processing of his personal data; in particular due to the operation of their new marketing tool, D.

The third item may be tackled in a number of ways, but a *good* answer would remark on some of the rights directly that can be exercised directly against PC, and/or the powers that a DPA might be in a position to wield in response to a complaint by B. The extent to which an answer is *very good* or *excellent* depends on the quality and comprehensiveness of their advice to this end.

On rights exercisable against the controller, rights to rectification (Art 16), erasure (Art 17), restriction (Art 18), right to object (Art 21(1)), the right to object to direct marketing (Art 21(2) and (3)), and the right not to be subject to a fully automated decision (Art 22), withdrawal of consent (Art 6(3)) may be applicable depending on how the facts are interpreted. However, there are certain pitfalls that markers should be wary of in arriving at a grade. For instance, it appears as though PC is relying on consent to justify its various forms of processing; therefore, a response that suggests the right to object under Article 21(1) should note that this is not relevant if PC is indeed relying on consent as a legal basis.

On the powers of the DPA, there are several DPA powers enumerated in Article 58 GDPR that may be relevant; particularly Article 58(2)(c), (d) and (f) that, in different ways, may enable the relevant DPA to force PC to stop its targeting activities.

As justification for the exercise of these powers, and indeed the right to restriction under Article 18(1)(b), various of PC's problematic activities might be argued as unlawful under the GDPR, such as:

- likely issues with various principles, including 5(1)(a) lawfulness, transparency (given the lack of information seemingly given to data subjects, including relating to automated decision-making), and fairness (particularly given that B has opted to self-exclude from gambling in an attempt to overcome his addiction); (b) purpose limitation; (c) data minimisation and (2)(d) accountability; the lack of a DPIA undertaken by PC under Article 35 GDPR;
- the dubiousness of consent as a lawful basis for processing, especially given the 'all or nothing' choice presented to data subjects; and
- seeming disregard of data protection by design and by default under Article 25.

Question 2 (30%)

Consider the following variation of the scenario in **Question 1**. Rather than PuntClub implementing their marketing strategy themselves (i.e. in-house), PuntClub's "Discrimin8" tool is created, trained, and implemented by a big data analytics and artificial intelligence firm, Scrupeless (**S**), that conducts all of its activities from its office in Vietnam. According to a contract between the two, Scrupeless is to 'run PuntClub's online marketing operations as they see fit, with the goal of maximising user engagement and PuntClub's revenue.'

In order to build and operate Discrimin8, Scrupeless has complete access to PuntClub's data, including PuntClub user data. However, the storage of this data remains on PuntClub's private servers in the EU at all times. In other words, Scrupeless builds and implements Discrimin8 remotely, with none of PuntClub's data stored on Scrupeless' servers in Vietnam.

Briefly advise PuntClub whether, under the GDPR, (i) this arrangement constitutes a transfer of personal data to a third country under the GDPR; and (ii) whether PuntClub and/or Scrupeless are controllers or processors. It is not necessary to consider whether any transfer of personal data to a third country is lawful.

The point of (i) is to have Master's students engage with an area of uncertainty under the GDPR. A *good* answer would note that the term 'transfer' is not defined in the GDPR, however, it was considered (albeit in a different context) in Case C-101/01 *Lindqvist*. A *very good* to *excellent* answer would reflect on whether the relatively pragmatic decision arrived at then would continue to hold today, especially given recent case law on TBDFs that arugably has given primacy to fundamental rights (e.g. *Schrems I* and *Opinion 1/15*). An *excellent* response might also mention the EDPB's view that 'remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA, is also considered to be a transfer': see EDPB, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'. It is not necessary to refer to academic literature on point (e.g. Esayas' article 'A walk into the cloud', which was mentioned in lectures) but students should be rewarded for doing so. It is reasonable to conclude either way on this issue.

Question 2(ii) is intended to prompt students to consider some of the relatively recent case law from the CJEU regarding the scope of controllership and joint controllership. For instance, Case C-25/17, *Jehovan todistajat*, Case C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, and Case C-40/17, *Fashion ID*; and not least of all Case C-131/12, *Google Spain*. A *good* answer would discuss the basic requirements of controllership under Article 4(7) GDPR, being the entity that 'alone or jointly with others, determines the purposes and means of the processing of personal data'. A *very good* response would critically analyse the roles of both PC and S; whilst the former is determining the purposes of processing, there is a thin argument that they are blind to the 'means', given S is given full autonomy to build D as they see fit. Conversely, a similarly thin argument could be made that S is only determining the means, not purposes. An *excellent* answer, however, would refer to recent case law emphasising the protection of fundamental rights in determining controllership; reducing the responsibility of either PC or S would be problematic to that end, and

therefore, both are likely to be deemed joint controllers for the purposes of processing of personal data through the D tool.