**EXAM PAPER**

**JUS5630 - Privacy and Data Protection (MA)**

**Spring 2019**

There are 7 exam questions. The answers to questions 1, 2, 3, 4 and 7 together account for 65 percent of the overall grade for the exam. The answers to questions 5 and 6 together account for 35 percent of the overall exam grade.

The language of examination for this course is English: students may answer in English ONLY, answers in any other language than English will be given an F (F for fail).

Introductory guidance notes:

The exam is not especially tough; thus, there is no need to be extra-generous in grading the answers. The exam involves undertaking a fairly perfunctory analysis and application of the GDPR in respect of a relatively straightforward hypothetical scenario. The exam is mainly testing students’ ability – under considerable time pressure – to pick their way through the GDPR, construe properly some of its central concepts, and identify potentially relevant provisions but without undertaking extensive analysis of these.

**Consider the following hypothetical scenario:**

A private hospital in Sweden stores its patients’ clinical data in cloud-based electronic health records (“EHR”), which are accessible through the hospital’s IT system. This means that the data are not stored locally on the hospital’s servers, but in data centers made available over the Internet by a cloud service provider. On average, the hospital treats around 1000 patients per year.

The cloud-based services for the EHRs used by the hospital are provided by HealthCloud, a company with establishments in several EU Member States, but whose data centers are located in the United States. To make use of these services, the hospital has entered into a data processing agreement with HealthCloud.

The hospital has set up its IT system in a way that allows any of the 70 physicians working at the hospital, regardless of their specialty, to access at any time the data of all patients in the EHRs. Several non-medical staff (i.e., nurses, IT administrators, social workers) are also given unrestricted access to the EHRs. In total, 900 users have unrestricted access to the EHRs. The hospital has not adopted any formal policy regulating the setting up of user accounts and privileges, nor has it appointed a data protection officer (DPO).

As a consultant with expertise on the EU General Data Protection Regulation (GDPR), you are asked to assist the new management of the hospital in assessing the hospital’s compliance with the GDPR. More specifically, in light of the GDPR, you must advise on the following issues and, in each case, provide reasons for your advice:

1. **Which of the parties (i.e., the hospital, HealthCloud) should be considered a controller or a processor with regard to the personal data in the EHRs under the GDPR? Please justify your answer and refer to the relevant legal provisions along with relevant case law.**

The relevant provisions are Articles 4(7) (defining ‘controller’) and 4(8) (defining ‘processor’). Both definitions are basically the same as under the Data Protection Directive (DPD), so CJEU case law and Article 29 Working Party (WP29) guidance on these notions as understood in the context of the DPD will be relevant for construing the notions in the context of the GDPR.

A good answer would qualify the hospital as controller and HealthCloud as processor.

1. **What legal bases are available to the hospital under the GDPR for the processing of the clinical data in the EHRs? Please justify your answer and refer to the specific provisions of the GDPR.**

A good answer would point out that the clinical data in the EHRs are special categories of data under Article 9(1) GDPR. Consequently, the answer would continue by discussing at least some of the following legal bases (ideally all of them):

* 9(2)(a) (“explicit consent”);
* 9(2)(c) (“vital interests of the data subject”);
* 9(2)(g) (“substantial public interest”);
* 9(2)(h) (“reasons of public interest in the area of public health”);
* 9(2)(j) (“scientific research”).

The scenario does not specify what are the specific processing activities carried out by the hospital. This should leave the students free to explore all of the above legal bases, and present a menu of possible options.

Please note that the processing of sensitive data always requires compliance with other provisions of the GDPR, in addition to those of Article 9. This raises the question of whether Article 9 constitutes a separate legal basis for data processing, or if it only complements Article 6 GDPR and therefore the processing has to be supported by a legal basis in Article 6 as well. In light of this, students may refer in their answers to Article 9 in combination with relevant legal bases in Article 6.

1. **Which provisions, if any, of the GDPR has the hospital breached, and why?**

A good answer would mention the following possible violations:

* A violation of Article 5(1)(c) (“minimization principle”) by allowing indiscriminate access to patients’ data to an excessive number of users.

The essential principle concerning access to an EHR must be that – apart from the patient himself – only those healthcare professionals/authorized personnel of healthcare institutions who presently are involved in the patient’s treatment may have access. There must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR record.

The hospital should have adopted a policy regulating which categories of healthcare professionals/personnel, and at which level, have access to EHR-data (e.g., surgeons, psychologists, nurses, etc.).

* A violation of Article 5(1)(f) (“integrity and confidentiality principle”) as a result of non-application of technical and organizational measures to prevent unlawful access to personal data in the EHRs.
* A violation of Article 32(1)(b) for failure to implement appropriate technical and organizational measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services of the hospital.

A very good answer would also:

* flag the possibility that Article 25 (particularly 25(2) dealing with data protection by default) has been breached.
* raise the need to carry out a DPIA in accordance with Article 35 GDPR. However, arguably, the factual scenario does not provide enough information to conclude on this point.

1. **What are the administrative fines that the hospital would be liable to pay, if its conduct is found to be in breach of the GDPR?**

Under Article 83(5)(a), the first two of the above-listed violations are punishable with a fine of up to 20 million euros or 4 percent of the total annual turnover of the hospital.

Under Article 83(4)(a), the third, fourth and fifth listed violations are punishable with a fine of up to 10 million euros or 2 percent of the total annual turnover of the hospital.

A very good answer would also point out that Article 83 GDPR establishes specific criteria for determining the actual amount of the fine to be imposed for a breach of the GDPR.

1. **Does the fact that HealthCloud’s data centers are located in the United States present specific compliance challenges under the GDPR? If so, which and how should these be appropriately addressed?**

A good answer would point out that the storing of patients’ data outside the EU presents transborder data flows challenges.

These challenges should be addressed by ensuring that HealthCloud has signed up to the Privacy Shield scheme; otherwise other appropriate transfer mechanisms should be followed (e.g., contractual clauses, express consent of the patients).

1. **Is the fact that the hospital has not designated a data protection officer problematic from a compliance perspective under the GDPR? Please justify your answer.**

A good answer should focus on whether the hospital processes personal data “on a large scale” (see Article 37(1)(c)). If it does, the hospital should have appointed a DPO.

A very good answer would refer to recital 91 GDPR according to which, on the one hand, ‘large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk’ would be included, in particular. On the other hand, the recital specifically provides that ‘the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer’. While it is not possible to provide an absolute answer on this point, the scenario at hand seems to be closer to the individual physician example in recital 91 (1000 patients per year is not much more than the number of patients that a regular GP would normally visit). Thus, it is likely that the hospital does not need to appoint a DPO.

1. **Assuming that the hospital would be a public one, could Sweden be held liable for the processing operations carried out by the hospital under other legal frameworks (beyond the GDPR)? If so, which? In your answer, you should refer to relevant case law, as appropriate.**

A good answer would refer to Article 8 ECHR. A very good answer would refer to the *I v Finland* case. In this case, the ECtHR found Finland to have violated its positive obligations to secure respect for private life pursuant to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), due to its failure to secure, through technological-organisational measures, the confidentiality of patient data in a public hospital.

A very good answer would also refer to Article 17 ICCPR.