**EXAM PAPER**

**JUS5630 - Privacy and Data Protection (MA)** - **Spring 2019**

There are 5 exam questions. The answers to each of the questions account for 20 percent of the overall grade for the exam.

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).

**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.

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.**
2. **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.**
3. **Which provisions, if any, of the GDPR has the hospital breached, and why?**
4. **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?**
5. **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.**