Please read the following case studies in advance of class. Some are a bit complex and it will help you to learn more if you familiarize yourself with them in advance. During the seminar, you will break up into groups and discuss each scenario for a few minutes. Then, one student will be asked to represent the group and share the group's response to the rest of the class. Discussion will follow. We will move through one question at time. We might have time to go through them all but we can try!

Case study 1: Fingerprint-reading devices

Cosmic Systems is a company based in Sweden that manufactures components for satellites. Citing general concerns about security, the company management decides to install fingerprint-reading devices to control all points of access to the company's manufacturing plant, where most of the company employees work. This means that all current and prospective employees of the company must have their fingerprints scanned and registered in a database.

Identify and discuss any data protection issues in this scenario. For example, do the employees have any rights with respect to these data? Are there any requirements for how these data must be handled?

Case Study 2: Medical files sent to incorrect email address

On September 8, 2016, Office of Doctor X discovered that an email containing a patient file had been sent to an incorrect recipient. This was the result of a typographical error when entering the email address. The patient file was exported from the software system used by the Office of Doctor X and attached to the email. The data controller became aware of the matter when the intended recipient contacted the data controller advising that they had not received the email.

What kind of data protection issues are highlighted in this scenario?

Case study 3: Controller vs processor

A) A gym engages a local printing company to produce invitations to a special event the gym is hosting. The gym gives the printing company the names and addresses of its members from its member database, which the printer uses to address the invitations and envelopes. The gym then sends out the invitations. Who is the controller and who is the processor? What are their responsibilities?

B) A GP surgery uses an automated system in its waiting room to notify patients when to proceed to a GP consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information. Who is the controller and who is the processor? What are their responsibilities?

C) Your company/organization offers babysitting services via an online platform. At the same time your company/organization has a contract with another company allowing you to offer value-added services. Those services include the possibility for parents not only to choose the babysitter but also to rent games and DVDs that the babysitter can bring. Both companies are involved in the technical set-up of the website.

Case study 4: Substantive scope

Kerstin is the daughter of Ellen. Unfortunately, Kerstin is no longer on speaking terms with her mother because Ellen posted numerous pictures of Kerstin's three, underage children on Facebook and Instagram. Kerstin has made several requests for her mother to take down the pictures of her grandchildren since she does not want them to be on social media. Ellen refuses since she has a very special bond with the children and she has helped to raise them.

Is Ellen obliged under the law to remove the photos of her grandchildren from social media?

Case study 5: Right to be forgotten

Hans orders goods from Company X on October 5. On October 6, Hans asks Company to delete his personal information. However, Company X needs his information to complete the order. Must Company X delete that information upon request? Why or why not?

Case study 6: Data portability

Elsa gets an application that will help her track her finances called Tinker. She completes an online form to set up an account with the app company and provides Tinker with her phone number, address, etc.

Through the App, Tinker is able to observe data about Elsa, such as her location. Tinker is also able to make inferences about Elsa based on further analysis of the personal data provided by Elsa (e.g credit score).

What data is subject to the right to data portability? If Tink receives a request from Elsa, how can it really be sure that is in fact Elsa and not someone trying to steal her personal data?

Case study 7: Data transfers I

A Swedish company uses a centralized human resources service in the United States provided by its parent company. The Swedish company passes information about its employees to its parent company in connection with the HR service. Is this a restricted data transfer under the GDPR?

Case study 8: Data transfers II

Personal data is transferred from a controller in France to a controller in Sweden (both countries in the EEA) via a server in Australia. There is no intention that the personal data will be accessed or manipulated while it is in Australia. Is this a restricted data transfer under the GDPR?

Case study 9: Lawful grounds to process personal data

Stockholm City Hospital wants to introduce a data loss prevention application to scan the entity's entire email traffic for possible leakage of sensitive health data. Is this permissible?

Case study 10: Lawful grounds to process personal data

A hairdresser conducts a patch test on a client to check that they will not have an allergic reaction to a hair dye. The hairdresser records when the test was taken and the results. Is this compliant with the GDPR? What kinds of information security concerns raised in this scenario?

Case study 11: Data Anonymization

For its upcoming 20th anniversary, a private tuition service provider wants to find out how many of its former students attended a university and, if so, what they studied. For this purpose, the service provider collects the data of its students from the past 20 graduation years and contacts them via email to participate in an online survey. In order to anonymize the data, the survey does not contain questions on the name, email address, graduation year or date of birth. The IP addresses of the participants are not being recorded. Furthermore, in order to avoid the identification of former students who graduated in more unusual study subjects, the latter are being regrouped into study areas, such as 'natural sciences', 'legal and business studies', 'social and educational studies' and 'language and cultural studies'.

Identify whether you think this data set is sufficiently anonymized in order to avoid the application of the GDPR.

Case study 12: Territorial scope

Entity I is located in the US and runs a portal for peer-to-peer holiday apartment rental. Via I's website, customers from around the world can rent out their apartments to tourists. In order to offer an apartment on I's website, each person needs to open a user account and enter a number of details, such as the name and the address of the apartment. I stores this user data. If a person calls up the website, it will be redirected to a website corresponding to its IP geolocation data. If, for example, the user selects 'France', the website appears in French language and the domain name changes from 'I.com' to 'I.com/fr'. Rental prices will then be indicated in euro instead of US dollar.

Case study 13: Data minimization

Entity D is a large car producer. Its HR department recruits new employees to expand the business. The applicants' CVs are used to assess their potential for the open job positions. The CVs contain, among others, the personal details and contact information of the applicants, their previous work experience, education, qualifications and skills. D set an application deadline. When D receives an application, the date of receipt is automatically stored, together with the respective application.

How can Entity D apply the data minimization principle in this situation?

Case study 14: Automated decision making

X Company produces personalized advertisements based on profiling. Sally complains to Company X contending that she does not want to subject to an automated decision. Must Company X comply?

Case study 15: Legality

The Royal Swedish Tennis Association ("RSTA"), located in Stockholm, Sweden, sold the personal data of more than 10,000 of its members to sponsors who had contacted some of the members by mail and telephone for direct marketing purposes. RSTA sold personal data such as name, gender, telephone number and address.

You work for the Swedish Authority for Privacy Protection (IMY). Decide whether to impose fines and if so, on what basis.