ES1: Ethics and Legality

2026-03-06

Table of contents

> ! Examination
>
> This seminar is mandatory and active participation is required to pass the course!

Seminar Structure

Approximately 5 groups with approximately 4 students each.

Part 1 (2 * 45 min)

Group discussions. Each group discuss the scenarios in different orders. Don't rush through all but spend as much time as you think is relevant on each of them.

Part 2 (45 min)

Classroom discussion. Each group present their discussion, interpretation and conclusions.

Discussion order

There are 7 scenarios described below. Each group take them in the order described here (starting with the scenario matching the group number, continue to the end and then from the beginning):

- **Grupp 1:** 1, 2, 3, 4, 5, 6, 7
- **Grupp 2:** 2, 3, 4, 5, 6, 7, 1
- **Grupp 3:** 3, 4, 5, 6, 7, 1, 2
- **Grupp 4:** 4, 5, 6, 7, 1, 2, 3
- **Grupp 5:** 5, 6, 7, 1, 2, 3, 4
- **Grupp 6:** 6, 7, 1, 2, 3, 4, 5
- **Grupp 7:** 7, 1, 2, 3, 4, 4, 5

(There would probably be less than 7 groups in total.)

> ! Time planning
>
> The difference scenarios varies in length! Don't get stressed if you start with a time-consuming scenario. If you have a lot to discuss, it might be enough to discuss just a few scenarios. Quality before quantity!

Instructions

This is not a mathematics exercise. There are no single correct answers to the questions you will discuss.

The purpose of this seminar is to explore tensions between legality, ethics, professional responsibility, organizational constraints, and personal circumstances. Something may be legal yet ethically questionable. Something may be ethically appealing yet unlawful. Your task is to explore these gray areas.

> i GenAI?
>
> You are allowed to use generative AI during discussions but if so, also reflect on this short 2 page paper (4 pages incl references): Bias Legal Data for generative AI. The paper focus on criminal/civil law. It is possible that administrative law is not affected the same way. What do you think?

- Work in groups of four.
- For each scenario, each of you must argue from the perspective of one assigned role.
- Assign roles randomly.
- Rotate roles for each new scenario (or after let's say 10-15 minutes; the aim is to lete everyone have each of the roles).

- You must argue from your assigned perspective — even if you personally disagree.

The goal is not to "win", but to understand how different values, pressures, and institutional frameworks shape decision-making.

When relevant, explicitly refer to:

- GDPR and its different parts
- The concept of data controller and processor
- The Freedom of the Press Act (Tryckfrihetsförordningen, TF)
- The Public Access to Information and Secrecy Act (Offentlighets- och sekretesslagen, OSL)
- Other relevant laws and regulations listed in the handouts/presented in EL2 and EL3

Roles

Justice Warrior

The rule of law is the foundation of society. Laws must be followed strictly, even when inconvenient. You are knowledgeable about legal structures and precise when referring to specific regulations. If an action violates GDPR, TF, OSL, or any other laws or regulations, including internal policies, it must not be taken — regardless of good intentions!

Burnout Statistician

You are officially employed for 40 hours per week but regularly work twice that. Deadlines are unrealistic and resources limited. You are exhausted and under personal stress. You want to do the right thing — but you are close to your limits. Practical survival sometimes outweighs ideal compliance.

The Idealistic Reformer

Your primary concern is improving outcomes for patients and society. Bureaucracy can stand in the way of meaningful progress. If rigid compliance prevents real-world benefits, you are willing to challenge procedures. Ethics and impact matter more than formalism.

The Budget Guardian

Public resources are limited. Every action has financial consequences. Legal violations can result in heavy fines, reputation damage, and loss of funding. You focus on long-term sustainability, cost-effectiveness, and institutional risk.

Scenarios

Scenario 1: The Data Receiver

You are participating in consultancy work through Akademistatistik.

A client from the Sahlgrenska Academy (University of Gothenburg) is conducting research where the Västra Götaland Region is the research principal (forskningshuvudman).

After an initial meeting, the client emails you a non-encrypted Excel file. The first column contains Swedish personal identity numbers (personnummer).

Discussion

1. What are your immediate reactions — legally, ethically, and practically?
2. Does the transfer itself constitute a personal data breach under GDPR?
3. What risks are involved (for individuals and institutions)?

Suppose the client used his `xxx@gu.se` address to send the file.

4. What does this mean in practice? Identify which organizations may now be involved in the incident.
5. Under GDPR, who is likely the data controller? Could there be joint controller-ship? What role does Akademistatistik have?
6. What obligations arise immediately (documentation, reporting, internal notification)?

You find the following text on the GU intranet:

> A personal data breach is a security incident that can involve risks to human rights and freedoms. Everyone at the University of Gothenburg has an obligation to report incidents that they discover to the Data Protection Group. A personal data breach has occurred if, for example, data concerning, one or several registered persons have been destroyed, got lost in any other way or made available for unauthorized persons. The risks of a personal data breach can include loss of control over data or the restriction of people's rights. A personal data breach is therefore a security incident that has affected the confidentiality, accuracy or availability of data. A personal data breach may consist of: An unauthorized party has gained access to the personal data, for example by sending personal data to recipients who should not have the data. […] The University of Gothenburg is responsible for the incidents that occur within the university's activities. The head of the part of the organization where the incident occur must ensure that the incident is reported, managed and assessed. When you discover a suspected personal data breach at the University of Gothenburg, you must report it within the organization as soon as you become aware of it. You do this by emailing dataskydd@gu.se with a copy to the closest superior college. The Data Protection Group will then initiate documentation and assessment of the breach. It is very important that any incident is reported swiftly, as serious breaches must be reported to the Swedish Authority for Privacy Protection (IMY) within 72 hours of the incident being discovered. The 72 hours is the time that the Data Protection Group and the Data Protection Officer have to make their assessment of the incident.

7. What do you do now — concretely and immediately?

Instead, imagine that the researcher used `xxx@vgregion.se`.

8. Would that change anything? Consider controller responsibility, breach notification, and organizational accountability.

Later, at a restaurant, you mention receiving the file. A person nearby asks you to share the data. You refuse. He claims that since you work for a public authority, the Freedom of the Press Act (TF) gives him the right to access the document immediately.

9. What is your response?
   - Is the Excel file a public document?
   - Does secrecy under OSL apply?
   - Who decides on disclosure?

Scenario 2: Working with Data Across Borders

You are hired remotely by a company in Moldova. You have not yet received a work computer. Sometimes you work from cafes or libraries.

The company has a Swedish client who is the data controller. You download their data from an encrypted server connection.

Discussion

1. Before starting work, what technical and organizational safeguards must be in place?

Suddenly, the client realizes that no Data Processing Agreement (DPA) exists between them and your employer.

Your boss says: "Not my problem. GDPR does not apply to me."

2. Is that correct?
3. What is your professional responsibility?
4. Do you continue working?

Scenario 3: Secure Environment

You must work in a restricted remote server environment.
You cannot install packages outside CRAN.
You cannot copy text or files.
The client can only access your final reports (results/tables/figures etc) directly on the server.

You urgently need a GitHub package not available on CRAN. You discover a technical workaround to install it despite restrictions.

Discussion

1. Do you use the workaround? Why or why not?
2. Is bypassing IT restrictions merely a policy violation — or potentially a legal issue?

Later, you discover you can activate AI tools externally to assist your analysis. You are severely sleep deprived and under pressure.

3. Do you use AI tools?
4. Could this involve unlawful data transfer outside the EU?
5. How do exhaustion and working conditions affect ethical responsibility?

Scenario 4: The Accident

You work for a national quality register of joint replacements. Late one evening, a hospital calls you:

> "We have a severely injured patient. His face is unrecognizable, and he is unconscious. We cannot identify him. However, his hip prosthesis is exposed and we have located the serial number. If we can identify him and access his medical history, we may be able to save his life."

The hospital asks whether you can use the register to identify the patient based on the prosthesis serial number and provide identifying information.

Discussion

1. Are you legally allowed to disclose identifying information?
2. What is the original purpose of the register, and does this situation fall within that purpose?
3. If not, is it still possible to provide the information?
4. When, if ever, should privacy yield to immediate medical necessity?
5. Would you make the same decision at 10 a.m. on a weekday as at 2 a.m. when you are alone?

Variation

Imagine that: - The patient survives regardless of your decision. - Later, relatives question how the hospital obtained identifying information. - Media becomes aware of the incident.

Does this change your reasoning in retrospect?

Scenario 5: The Role Model

You are relatively new at your workplace. A senior colleague has taken you under his wing, helped you understand internal systems, and supported you in difficult projects. This colleague is widely respected, seen as highly competent, and something of a role model in the organization.

One evening, you are working late. While navigating a shared network folder for a project, you come across several script files. Out of curiosity — and because the file names seem related to a database you recognize — you open them.

The scripts clearly show that your colleague has performed a data extraction containing names, personal identity numbers, and addresses for all individuals living on the same street as him.

There is no obvious documentation justifying the query.

Discussion

1. What are your immediate reactions?
2. Does this appear to constitute:
   - Unlawful processing under GDPR (lack of legal basis, purpose limitation)?
   - A personal data breach?
   - Possible misconduct or even a criminal offense (e.g. breach of confidentiality)?
3. Does it matter whether the data was merely accessed, or also exported and used?
4. What risks arise for:
   - The affected individuals?
   - The organization?
   - You?

Further Considerations

5. Do you confront your colleague?
6. Do you report the incident internally? If so, to whom?
7. Are you yourself at risk if you ignore what you have seen?
8. How does the power imbalance (junior vs senior) affect your responsibility?

Scenario 6: Contacting Children from a Quality Register

You are the head of a unit responsible for a national quality register for children born with cleft lip and/or palate.

You receive a formal data access request. The researcher has an approved ethical review decision from the Swedish Ethical Review Authority (Etikprövningsmyndigheten).

The researcher requests access to identifiable personal data (names, personal identity numbers, and contact information) for children living in Western Sweden. The stated purpose is to contact the children and their guardians directly to invite them to participate in a new research project involving follow-up questionnaires and interviews.

Discussion

1. Does the purpose of the quality register allow this type of secondary use?
2. Does an approved ethical review automatically mean that the data may be disclosed?
3. Does the age of the children matter (minor vs adult at time of contact)?
4. What are the ethical implications of contacting families about a condition that may carry psychological or social sensitivity?
5. Does secrecy under the Public Access to Information and Secrecy Act (OSL) apply?
6. Are there any personal risks for you if you accept to give the researcher the data?
7. Will you accept or decline the request?

Variation

Imagine that:

- The researcher is well-known and highly respected.
- The project has strong potential to improve long-term care.
- The researcher argues that obtaining consent indirectly will drastically reduce participation rates.

Does this change your decision?

Scenario 7: Unreasonable Promises?

Read about the Gothenburg Study of Children with DAMP (the abbreviation was used at the time but has since become outdated). Focus on the section “Allegations and destruction.”

Tip

You are also recommended (although it is not mandatory) to read this BMJ Feature. However, please do so after the seminar (or beforehand if you happen to come across this text in advance, since we will not have the time during the seminar). It is an interesting case and may provide some additional insights in the grey-area between legality, ethics and research practice.

As a side note, the Church of Scientology's involvement in relation to Sweden's Freedom of the Press Act and public access to official documents is also an interesting topic in its own right, although most discussions of it are available only in Swedish.

Background (Summary)
In brief:

- Researchers collected highly sensitive data from children and their families.
- Participants were given strong assurances that their privacy would be protected and that the data would not be shared outside the research group.
- The scientific validity of parts of the research was later questioned.
- External researchers requested access to the original source material in order to replicate or scrutinize the findings.
- The University of Gothenburg refused to disclose the material.
- The external researchers appealed to the Administrative Court of Appeal ("Kammarrätten"), which ruled in their favor but accepted ten conditions set by the university for access.
- The researchers in possession of the data appealed to the Supreme Administrative Court ("Regeringsrätten", now "Högsta förvaltningsdomstolen"), which did not overturn the decision.
- The requesting researchers also appealed, objecting to some of the conditions; a later ruling further strengthened their right of access.
- The researchers holding the material destroyed the data rather than disclose it.
- The destruction of the data was ruled illegal.
- The responsible researcher was fined and received a suspended sentence.
- The university rector and additional researchers (including the wife of the responsible researcher) were also convicted and fined.
- The responsible researcher filed an application with the European Court of Human Rights in Strasbourg, arguing:

> In my view, it is unreasonable that I am first obliged to give strict promises of confidentiality by the State in order to conduct medical research, then… I am ordered by the State to break hundreds of promises of confidentiality…then am sentenced as a criminal by the State because I had not broken those promises of confidentiality. "Something is clearly wrong in this chain of events, but it is difficult to see how the error can be mine."

- The European Court of Human Rights rejected this argument.
- The researcher remains active and successful within his academic field.

Legal Context

These events took place approximately 20 years ago, before the GDPR entered into force (although the Swedish Personal Data Act, PUL, was in effect at the time). The current Public Access to Information and Secrecy Act (Offentlighets- och sekretesslagen, OSL) was enacted later.

For the purposes of this discussion, base your reasoning on **current Swedish and EU legal frameworks**.

Discussion

Feel free to choose among those questions if you don't have time to discuss them all:

1. Can researchers promise absolute confidentiality in a country with strong public access to official documents (offentlighetsprincipen)?
2. If a public university is the data controller, who ultimately decides whether data must be disclosed — the researcher, the university, or the court?
3. Does an ethical approval and informed consent override obligations under freedom-of-information legislation?
4. Under current GDPR and OSL:
   - Would disclosure of identifiable research data be possible?
   - Under what conditions?
   - Would pseudonymisation change the legal assessment?
5. Was the destruction of data ethically defensible, even if illegal?
   - Is it ever justifiable to break the law to protect research participants?
   - Does intent matter?
6. How should conflicts between:
   - Research integrity (replicability and transparency)
   - Protection of vulnerable participants
   - Public access to documents
   - Legal compliance be balanced?
7. Could the promises made to participants have been formulated differently?
   - Should researchers in public institutions avoid absolute guarantees?
   - Is "maximum protection within the limits of the law" a more appropriate formulation?
8. Who carries the ultimate responsibility in such cases?
   - Individual researchers?
   - University leadership?
   - The legal department?

9. Consider a modern parallel:
    - Suppose a similar dataset existed today under GDPR.
    - Would the legal outcome likely differ?
    - Would reputation consequences differ?
10. Is the European Court's rejection of Gillberg's argument legally unsurprising?
    - Or does it reveal a structural tension between research ethics and public law?