ES1: Ethics and legality

Data receiver

Imagine that you are participating in consultancy work through Akademistatistik. At the meeting, a client is present who is employed at the Sahlgrenska Academy at the University of Gothenburg, but who is currently working on a research project in which the Västra Götaland Region is the research principal (”forskningshuvudman”). After an initial start-up meeting, the client gets in touch and asks for help with analyses of the collected data material. In the email, there is an attached non-encrypted Excel file, and the first column contains the personal identity numbers of all individuals.

1. Describe and discuss your initial thoughts on this situation.

Suppose the client used his xxx@gu.se-adress to provide the data.

2. What does this mean in practice? Identify the three organizations which now have acces to the data.
3. Acording to GDPR, which organisation is the data controller and which roles do the other organizations have?

You search for some help and find this text on the GU intranet (as published 2026-01-19):

> 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 unauthorised 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 unauthorised 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 organisation 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.

4. So what do you do now?

Instead, imagine that the researcher used his other e-mailadress xxx@vgregion.se.

5. Would that make a difference? If so, how?

Let's say you do not take any action in this case. At a later dinner with some friends at a restaurant, you talk about the project and mention the Excel file you received. Someone at a nearby table hear what happened and ask you if you would like to shere the data with him.

6. What is your response?

If you decline, he might insist that since you received the data as a "representative" for the University (a govermental institution), the freedom of the press act (TF) does give him the right to "demand" that you give him the data as soon as possible.

7. What do you do now?

Working with data

Imagine you just got hired as a statistician working remotely for a company in Moldova. You have not yet recieved any computer from your employer. You don't want to sit home alone all the time so sometimes you work from a library or a café. The company has a Swedish client wich is the data controller. You can download their data from a secure server and that connection is encrypted.

1. What are the first practical things to consider before you start working with their data? What is your reasoning?

Suddenly, the clients realise they had not established any formal Data Processing Agreement between them and your employer. You ask your boss for advice, but she doesn't care. "Not my problem, GDPR does not apply to me!"

2. What do you do?

Secure environment

At your work you are forced to work with your data only on a remote server. R is installed but you can only install packages from CRAN and you can not copy any text or files between the server and your computer. You need to finish a report for the next morning (the client can access the report himself on the server). The only possible solution you can think of is to use a newly developed R package available on GitHub. Although you can not install such packages through the restricted R environment, you have found a clever way using some undocumented procedures using the command line one the server.

1. What do you do?

After some additional experimentation you find out that you can even activate AI tools to help you with your work. In fact, you haven't slept for three days, your boss doesn't pay you enough and the report must really be finninshed tomorrow.

2. What do you do?

The accident

You are working for the national quality register of joint replacements. One day you receive a call from the hospital. "We have a seriously injured person here. His face is unrecognisable and we don't know who he is. But his hip prothesis is sticking out of the body and we have a serial number. We might be able to save his life if you can identify him and we can look into his medical history".

1. What do you do?