RIKSREVISIONEN

Ange avdelning

Intervju KTH11 21 februari 2023

Prefekt Skolan för kemi, bioteknologi och hälsa

Från RiR: Sara Monaco och Ludvig Stendahl

Inledning

What does a normal week look like?

Approx. 1/3 management, 1/3 own research, 1/3 teaching. But it varies over weeks. Teaching involves adm, preparing lectures, evaluation, grading. Research contact with postdocs, on Friday I will be opponent at dissertation. As Head of dep I sign contracts, help people trouble shoots small problems, I have meetings with faculty members... It is very diverse, our tasks are so diverse, it makes it fun. The reasons why I'm here. Otherwise I would have stayed in industry.

Is this mostly applied research?

Both. We are interested in use and industry, but we also want to understand how things work. Some of the research might be close to application, some research might be 10 years away.

Utformning av informationssäkerhetsarbete

How do you work with info security as Head of dept?

The main role is to think before we start projects if it's relevant or not. We don't have much patient data, GDPR only deals with our own personal info, we can ask HR. Other data... we don't have state sensitive topics, no military. We have collaboration with companies, might be confidential during a period during the research. Important how you share info, we rely on the it-dept. here, it's good that that it's centralized at KTH.

How do you work with info.security at your dept?

It's often discussed, mainly within the research teams. If there are questions, they can be discussed with me. Equally important that data is of good quality so that we can share it.

You might have state sensitive data?

I have never been in that situation, but of course it might happen...

Are there different challenges, do you have local challenges here at the dept? How do you lift them to higher level?

Apart from lifting to the it-dept? We have monthly board meetings, open contact with the Head of the school. It would be an open discussion. I would first contact it-dept. Let's say that I have a researcher who wants to use patient data, I would know where to find info...

Is info security a topic at school dialogues?

No.

We have monthly board meetings at the School level, all head of depts and adm. We also have meetings where all faculty members discuss.

We also have monthly dept meetings.

Roller och ansvar

What is your role when it comes to info security and is it clear to you what responsibilities you have?

The role if formally the head of school and rektor level, but I also feel responsible, if anything is unclear. The individual PIs have to take responsibility.

Do you have a supervisory role?

PIs are responsible for data to be available, I have an important check in role to see that it goes well with eg GDPR

How do you do that?

I make sure to have good contact with PIs, open communication.

Is there someone responsible for info security at dept level?

In practice I would contact our contract manager at school level, or head of school. We keep lines very short. The school contract manager looks at all contracts, she has to be involved, many contracts are signed by head of school.

Is data handling included?

More and more, VR demands it. Formas as well. Historically it was not so much.

Do you find data management plans helpful?

It's not much work to fill them in, just "state the bloody obvious" as the British say. No problem.

Both Sweden and X go in the same pace, very similar. It's more about sharing data etc, we did not do that 20 years ago.

If you collaborate with industry?

The contract would always be for a project. One of my colleagues has center of excellence, funded by Vinnova, it includes collaboration with 10 companies. You might have two contracts, one with VR and one with the company, with different rules. Be careful not to mix them. You need a data management plan for each project. Project management becomes crucial in those cases.

Interna regler och arbetssätt

Riskanalys och riskhantering

How about risk analysis at the dept? Is research data included there?

Risk analysis in general with do a lot, in the lab we work with chemicals, steam, dangerous fluids etc. Data security risk analysis we do when writing contracts, starting projects. Is there patient data y/n, state sensitive research y/n, companies confidential y/n, share data y/no. Individual researchers take part in this. If PIs come to me for approval I can ask them if they have dealt with certain things.

Is there a general risk with data management?

Your data should no be easy to hack for competitive reasons. Many countries would like to have the ideas. For the lab work we have safety managers

For research data is confidentiality the main risk?

Yes, and that others get data before we publish. At other depts there might be patient data.

Do you know all research that is conducted here?

Yes. And if I don't know I have to set up divisions. We are not that size yet. I know the data here.

Do you keep all data here, also when you collaborate with eg companies?

Yes, the exception would be that I might have an industry doctorand and the data might be at the company.

Other depts say the data are kept at the company?

Then it should not be research...? Should be contract research. In X 20 years I worked in a public partnership. The govt funding was used to fundamental research, companies paid to apply. These worked really well. It can be difficult to mix. You need to be very careful.

The work is so different between depts. How much external funding do you have, we've heard others having 70%.

We need the external funding, CBH school very important, even more than 70%

Informationsinventering och informationsklassning

According to you own KTH rules you should classify info, is this done here?

If it's confidential. Otherwise no. open data is not classified.

Is this documented? Or do you mainly talk about it?

The PIs that have these projects, they have a discussion in the research team,

Are the guidelines helpful?

For risk analysis yes, once a year it's good to think about these things. In practice we do it well, but formally it's not implemented yet.

If your department was bigger, how would it work?

Then I would need divisions...

Do you think size is a factor when working with infosecurity?

No, but I would need divisions.

Is the work mainly trust based?

Yes, but we also have formal checks when signing contracts, which is not trust based. You should have some formalities, but also trust based, that is good.

Internt stöd

Is the support from central level clear?

I think it's sufficient, especially at school level. Sometimes it's not obvious but on this topic I think it's ok. When GDPR entered we got a lot info.

Do you have contact with RSO?

They're essential, we have a lot of contact with them.

Utbildning, kunskap och kompetens

Is there training on information security?

With GDPR we had.

Efterlevnad

Do researchers follow policies and guidelines?

The vast majority yes. They might use parallel equipment, this isn't anything I can't guarantee...

Säkerhetsåtgärder

Does KTH have a secure storage?

The it-dept takes care of it. The location is the same, we have Microsoft one drive, and local networks solutions. We have a Scandinavian server for zoom.

Can you ask for separate equipment?

Yes at school level. I never had contact with the central it-dept.

Can you find data from finished projects?

Yes so far, but could be a challenge if format changes. In X 10 years ago I had problems.

Utvärdering och anpassning

Externa samarbeten

Do you sign contracts as Head of dept?

Some shorter contracts, otherwise it's the School head.

Bakgrundskontroll

If there are new people coming, how do they learn about info security?

Important introduce our rules,

Do you check visitors that are coming?

There are some grants that come from other countries, is this ok? Sweden as a country, I think we are a bit naïve. What does the Swedish govt think about these scholarships. They take data. The govt should deal with this naivety.

But research should be open?

Yes, but it's very different from being naïve

How have you dealt with these issues?

We have CDC-students, they might take data, but it's not sensitive data. We need to do it nationally, have national rules if the govt deems that it's needed.

Do you do background checks?

We don't do it since we don't have sensitive data. We check references, it is outsourced to a company to do it. It would be easier to do it myself. They don't answer when the company checking for references asks because they think that it's spam.

Incidenter (informationssäkerhet)

Avslutning

Is there anything that you think is missing, that prevents you from doing a good job on info security? Challenges?

No. A side from the national level. Maybe one thing, that all info should be available in Swedish and English. This is not always the case. It would be really beneficial, customer friendly in English. We did the same thing in X several years ago.

Has there been anything sensitive in this interview?

No.