RIKSREVISIONEN

Ange avdelning

Intervju KTH14 230227

Prefekter institutioner vid Skolan för industriell teknik och management

Från RiR; Sara Monaco och Ludvig Stendahl

Inledning

Infosäk, vad tänker du på?

B: Om vi har känslig data ska vi se till att skydda det.

Vad lägger ni in i begreppet?

Om vi har känslig data, tror inte vi har så mycket, så ska det inte hamna hos personer eller länder som inte ska ha den.

Hur jobbar ni?

A: Vi har en del säkkänslig data. Allt regleras i projektavtal, kan vara så att det inte ska delas.

X kan vara känsligt, hanteras i projektavtal. Där finns specifika NDA, vi ska inte visa all data.

Vi har ibland sekretessavtal, ibland i exjobb. Vi visar inte datan för andra. Tror att allt regleras via projektavtal. Våra jurister reglerar. Det är en avvägning mellan öppenhet och säkbehov. Ibland kan vi få säga till juristerna att det är ok att det är stängt. De jobbar alltid för att det ska vara så öppet som möjligt. Avtalen reglerar skyddsklassningen.

Går avtalen via er som prefekter?

A: Jo hos oss gör de det. Allt går genom CASE.

B: Allt går via CASE, vi skriver inte på alla. Det gör antingen skolchefen, eller vicerektor för forskning.

Beror på vad?

Om det handlar om företagssamarbeten, då försvinner det direkt från prefekten.

Har ni mest företagsparter?

A: Det finns andra också. Grundinställningen är att vi vill ha så lite hemlig info som möjligt. Sen kan vissa saker bli hemliga. När vi ska publicera tvättar vi bort lite av den data, eller så ändrar vi lite som inte industrin skulle göra. Vid exjobb kan vi publicera ett tvättad version.

Även industriexjobb?

A: Ja det är reglerat. Om det är hemligt, då diskuterades det vid början av proj. Tex hur man ska skriva i mejl för att man inte ska behöva tvingas lämna ut.

Och hur ser det ut inom X?

B: Vi har en del myndighetssamarbeten. Rymdstyrelsen, Ariane Espace, Sthlms stad. Alla har de sina regler som de skriver in i sina avtal.

Finns det standardförfarande?

A: Nej, men det brukar vara reglerat i avtal. Men om det är säkklassad finns inte datan online, bara på de personernas datorer där den används. Det är KTH datorer men inte tillgängliga via nätet, utan lagras på separat hårddisk.

Kan det skilja sig åt hur de ska hantera data?

A: Ja ibland kan det vara krav att bara européer får delta, eller att skydda data i 90 dagar.

Hur fungerar det i praktiken? Man vill kanske diskutera med kollegor?

A: Vi är öppna med det, såsom systemet är uppbyggt kan vi inte jobba med vissa. Vi är öppna med det.

Öppna hur?

A: Vi informerar vid våra avdmöten, informationsmöten, strategiska inst. Vi säger att vissa nationaliteter inte kan delta.

Även hos er?

B: Vi har samarbete med X; frågeställningen hamnar tillbaka hos X. Man frågar om den data som genereras av forskaren är säkklassad. Uppdragsforskning och industriparter. Hur man lagrar data, ren dator när man är ute och reser.

Brukar folk följa de riktlinjerna?

B: Den diskussionen är förhållandevis ny. Det har skett en stor förändring de senaste 3 åren. Vi har hela avtalsskrivningen, juristerna kommer in, med parten... de parterna vi har är otroligt strikta hur avtalet ska se ut. Vilka personer som ska vara involverade, det ligger på PL och handledaren. Avvägning, vi vill ju inte stänga. Vi vill ju publicera. Vi måste förhålla oss till det. Försöker göra på bästa sätt i enlighet med avtalet. Vi försöker vara långt från data som är känslig, vi kan göra det vi ska, företaget gör det de ska. I ganska många fall är vi inte i gränslandet.

Tycker ni att det är målkonflikt, öppenhet, tillgängliggörande? Som forskare prefekt?

A: De företag som är säkskyddsklassade, de är vana vid det. Har jobbat med flygforskning sedan 60-talet. Vana att jobba med högskolor, de hjälper oss med det. De tar hand om oss när det gäller den frågeställningen. Även när det gäller elnätet har de också bra koll. Jag känner inte att vi pga det inte har kunnat forskar eller publicera. Nästan mer målkonflikt när saker ska patenteras eller göras kommersiellt gångbart. Företagen har inget sätt att hantera det, det är svårare.

B: De hjälper oss, även i vissa fall gäller det företag som är rädda om sin info. Det är de som vet vad som är känslig data.

B: Vi använde data som är skyddsklassad. De säger ni kan publicera på det här sättet. Så att säkklassningen upprätthålls, och forskningen kan bedrivas.

Men startupföretag vet inte själva vad som behöver skyddas... de har svårast att hantera en sådan sak. De vill att vi ska vara ett slutet konsultföretag. De mindre har det svårare.

Uppstår det svårigheter ibland, är det alltid glasklart hur data får hanteras?

B: jag skulle bli förvånad om det var glasklart... vi är personer från hela världen med olika syn på det. Handledare... i vissa projekt kan man inte ha personer från vissa länder. Det är PL och handledarens ansvar. På doktorandnivå är det inte glasklart, det gäller att handlaren ser till att det blir tydligt för dem. Kan vara en ickefråga också, nåt generiskt, då diskuterar man inte det specifikt.

Men om det blir en aktuell fråga, kan det finnas osäkerhet där?

A: vi följer ju inte dagligdags upp att alla följer regler. Men PL måste ofta signera själv. Då blir man tvungen att uppmärksamma frågan. Jag följer inte upp personligen att alla följer avtalen.

Har ni avdchefer?

A: avdelningscheferna har delegation. Det är oftast de som hanterar den personliga kontakten med PL: De har ekonomiskt ansvar och styr projekten.

B: samma sak hos mig. Xx experimentell data, den ligger inte i molnet. Ansvaret hamnar på forskarna, lägga data på usb-minnet och ta det därifrån. Och att radera.

Har ni ledningsgruppsmöten? Disk ni infosäk?

A: Ja mer nu, men har diskuterat det även tidigare. Vi har haft fall där fel data gått ut till fel projekt. Vi har en uppföljning kring det. Nu brottas vi med hur vi skriver på NDA, är det ok att skriva på personliga NDA? Behöver alla gå över till juristerna? Idag går inte alla till juristerna. Skulle vara omöjligt. Exjobb kräver NDA, skulle bli så många. Vad ska skrivas på på central nivå och vad ska vara personligt?

Är det otydligt?

A: Nej, en avvägning man får göra själv. Begränsad – jag och avdcheferna tar det ansvaret med personliga NDA.

B: NDA är inte en stor fråga hos oss.- om frågeställningarna kommer upp tar vi dem i vår grupp.

Hur lyfter ni saker om infosäk till högre nivåer?

Jag skulle ta det med skolan. Juristerna.

Har ni dialog med skolan?

Vi har möte varannan vecka på skolan. På de ledningsgrupperna finns en öppen punkt där man kan ta upp vad som helst.

Har infosäk varit uppe?

Ja, absolut.

Har ni årliga kvalitetdialoger?

A: Ja, med skolan och KTH-nivå. Vi följer KTHs verksamhetsplan, skolans VP.

Hur tycker ni skolan lyfter infosäk till er?

A: Det är nog bra, via ledningsgruppen, via de återrapporteringskrav vi får. Det ligger mer mellan PL och jurister, mer en processfråga än en linjefråga. Då behöver det inte vara på skolnivå. Hur man skyddar ligger på ett annat ställe i processen.

B: får du ett projekt ska du fylla i en mall. Vi får mallar. Även info till juristerna. I CASE, vi ger informationen till dem så fyller de i.

A: Infon bearbetas av våra verksamhetscontrollers, de tar in den infon som kräv.

Verksamhetscontrollers, var sitter de?

På skolan men hör till skolans adm. Alla forskare måste gå den vägen.

Har ni lokal infosäksamrodnare på inst?

Nej, på KTH finns, inget lokalt. Det beror nog på att det är så projektstyrt. Mer projektstyrt än linjestyrt.

Annan säkerhet?

Inget lokalt. B: just nu bygger vi upp en lokal infrastruktur för vi behöver det, men det görs i dialog med centrala KTH-it.

Riskanalyser, har ni ngt process för det?

BL de flesta risker vi har är personrisker, skador i experimentella miljöer. All infrastruktur har riskbedömning. Även för avsked och anställningar. Oftast om arbetsmiljöfrågor.

Tas infosäk in i processen?

A: Ja i experimentella miljöer ja. Men inte i personfrågor. Säpo kan klassa ngn som började jobba med Svenska kraftnät.

B: jag har haft kontakt med Säpo när ngn ska anställas från vissa länder.

Har du haft kontakt med Säpo?

Nej, jag fick info från Migrationsverket gällde en doktorand, det drog ut på tiden.

Övergripande riskanalysarbete på skolnivå?

Nej... görs inget på skolnivå.

T ex klassa information...?

B: ja men alla data är inte känslig.
A: vi försöker ha det på den lägsta nivån.

Man måste ju identifiera det som är känsligt? Upplever ni att folk har koll som jobbar med känslig info?

B: Ja... men det kommer in i avtalet.

Är det ett bra system med avtal?

Ja för man kommer inte ifrån det. Tror det är mer verkningsfullt med en avtalsprocess. Diskussionerna med juristerna är bra, de vill att det ska fungera för KTH. Då blir det en förhandling automatiskt, och då blir det fokus på att göra rätt.

B: en stor del av avtalen går till juristerna, alla som inbegriper industri. Även sånt som har granskats,

Alla forskare skriver på avtal om man är med i centrumet. Ett forskavtal.

B: alla finansieringsavtal har NDA-komponenter i sig. Sedan finns det NDA som går utöver det.

Lagar som kan tillämpliga, PDA; OSL, säkskydd? Finns det reglerat i avtalen...?

A: Jag har inte full koll, jag delegerar till juristerna, ingen kräver att ngn ska ha full koll.

PDA, exportkontroll har varit aktuellt?

Ja det går till våra jurister. Flygforskning som jobbar med både civila och militära flygmotorer. Vi jobbar via nationella flygforskningsprojekten som tar hand om det.

Har ni koll på KTHs handläggare som jobbar med PDA, har ni haft besök av ISP?

Nej.

Är ni internationella? Hur hanterar ni det som det skrivits om i media på sistone?

Ja, om vissa nationer utesluts då är det så.

Har ni haft CSC studenter?

De har inte varit involverade i det som är känsligt.

B: vi har haft många, företagen har varit oroliga. De är med på vissa men inte andra. Men vissa företag tycker det är bra, då har man personer man kan anställa i landet sedan som har kopplingar till Sverige.

A: vi pratar om det på institutionen.

Finns det problem internationella rekryteringar?

B: Nej inte direkt. Ibland kan vi inte anställa vissa, det drar ut på tiden. Om det är förtagsparter involverade, vi skickar namn på kandidater. Jag skulle vara öppen för att de hade synpunkter på vilka vi ville rekrytera. Men det har inte hänt än.

Jag kollade publiceringar, samarbete med seven sons forskare. Hur tänker man som forskare?

A: jag tänker inte på att ett univ är styrt av militärt samarbete. Vår vice rektor har tagit upp den här frågan, vi har två partnersuniv i Kina. Vi utgår från att det finns en risk. På 90-talet var det Ryssland som var problem. Då fick vissa ryssar inte komma åt nätet.

Finns det otydligheter för er som prefekt eller forskare?

A: jag skulle vilja att uppdragsgivaren skulle vara mer tydlig: politiken och de som styr oss. Måste finnas balans. De får gärna vara tydliga FMV, Säpo, kring säkerhetsfrågor. Datahantering och personer.

B: bara positivt om det är tydligt. Vi har våra processer som tar hand om det. Det ändras med tiden. Nu kommer man fundera mer. För ett år sedan handlade det om ryska kopplingar, vi avslutade det som skulle avslutas. Vissa perioder har det varit Iran.

A: myndighetsdialog först. Blir det otydligheter då har det varit otydligt i myndighetssverige vad som gäller. Jag tycker vi är hyfsat duktiga på att fånga upp men om de inte är tydliga.

B: det kommer till oss från ledningsgruppen på skolan, som i sin tur hanterar på högsta nivå

A: Det behöver vara en iterativ process- diskutera - behövs alltid en dialog.

Webbutbildningar?

Ja tf säkerhetschef.

Vet ni om folk gått?

Nej det har fått inbjudningar men inte obligatoriskt att gå.

Datahanteringsplaner?

Nej de ser inte vi. Det är PL som ansvarar.

Om ni fick granska en sak som ni behöver mer hjälp med?

B: känner inte att jag behöver hjälp i de här frågorna. Vi har en process vi följer, även om den är förhållandevis ny.

A: det är kontinuerlig info från säkklassande myndigheterna. Personerna man nu har identifierat - de har ju forskat här i 5 år, då visste man ju det för 5-10 år sedan! Man hade det inte på radarn då? Lätt vara klok i efterhand. Om Säpo eller Must vill nåt får de säga det!