



Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Styrelsen

BESLUT

SLU ID: SLU.ua 2015.1.1.2-4473

2016-04-27

Rektor

Personuppgiftslagen

Beslut

Styrelsen beslutar

att fastställa internrevisionens rapport Personuppgiftslagen, samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

Ärendet

Internrevisionen konstaterar i sin rapport Personuppgiftslagen att det finns brister i hanteringen av personuppgifter vid SLU. Med anledning av detta rekommenderar internrevisionen ett antal åtgärder.

Beslut i detta ärende har fattats av styrelsen efter föredragning av universitetsdirektör Martin Melkersson. I beredningen av ärendet har även chef för ledningskansliet Miika Wallin och jurist Anna Jarmar deltagit.

Rolf Brennerfelt

Martin Melkersson

Kopia för kännedom

Prorektor

Dekanerna

Avdelningschefer (motsv.) inom universitetsadministrationen

Universitetdjursjukhusdirektör

Överbibliotekarie



Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

Internrevisionen

SLU ua 2015.1.1.2-4473

2016-04-27

Personuppgiftslagen

Rapport från internrevisionen

Innehåll

| | | |
|-----|--|----|
| 1 | Sammanfattning..... | 3 |
| 2 | Bakgrund och motiv | 4 |
| 3 | Granskningens omfattning och inriktning | 4 |
| 4 | Personuppgiftslag (1998:204)..... | 5 |
| 5 | Interna styrdokument för personuppgiftsbehandling..... | 6 |
| 6 | Hantering av personuppgifter inom SLU..... | 8 |
| 6.1 | Personuppgiftsombudets uppgift..... | 8 |
| 6.2 | Personuppgiftsbehandling utanför SLU..... | 9 |
| 6.3 | Personuppgiftsbehandling i forskning | 10 |
| | Bilaga 1. Regler som berör personuppgifter och säkerhet..... | 12 |

1 Sammanfattning

Syftet med personuppgiftslagen (1998:204) är att skydda den personliga integriteten vid behandling av personuppgifter. SLU är ansvarig för behandling av personuppgifter inom universitetet och ska besluta om vilka uppgifter som ska behandlas samt vad de får användas till.

Målet med granskningen är att bedöma om rutiner och processer för personuppgiftsbehandling följer gällande regelverk och är ändamålsenliga. Under 2015 har vissa förändringar i EU:s och Sveriges regelverk kring skydd av den personliga integriteten beslutats eller aviserats. Förändringarna har inte ingått i granskningen men aktualiserar vikten av att leva upp till nu gällande regler eftersom kraven kommer att skärpas under kommande år.

Internrevisionens sammanfattande bedömning är att följsamhet mot personuppgiftslagen brister, främst vad gäller delegation av ansvar, instruktioner och tillsynsuppgiften.

Brister i hanteringen kan medföra kränkning av den enskildes personliga integritet och leda till både förtroendeskada och ekonomisk skada för SLU.

De väsentligaste bristerna är:

- att det saknas beskrivning över ansvar och befogenheter att behandla personuppgifter enligt såväl personuppgiftslagen och etikprovninglagen,
- att det saknas tydliga anvisningar om hur personuppgifter får behandlas inom universitetet och
- SLU:s personuppgiftsombud utför inte samtliga uppgifter som åligger funktionen enligt personuppgiftslagen.

De väsentligaste rekommendationerna är i korthet:

- att ansvar och befogenheter för behandling av personuppgifter, enligt såväl personuppgiftslagen som etikprovninglagen, finns beskrivet i det interna regelverket,
- att instruktioner om hur personuppgifter får behandlas inom SLU finns tydligt beskrivet och
- att personuppgiftsombudets uppgifter utförs enligt personuppgiftslagen.

2 Bakgrund och motiv

Hantering av personuppgifter för att skydda människors personliga integritet regleras bl.a. i personuppgiftslagen (1998:204). Det finns även andra lagar som styr och begränsar hur personuppgifter får användas, exempelvis Lag (2003:460) om etikprövning av forskning som avser människor (etikprövningslagen). En av de stora utmaningarna när det gäller följsamhet mot lagstiftningen är den tekniska utvecklingen som möjliggör spridning av information samtidigt som kontrollen försvåras.

SLU har behov av att hantera personuppgifter i sammanhang som rör personal, utbildning och forskning. Enligt personuppgiftslagen är SLU ansvarig för behandling av personuppgifter inom universitetet och ska bestämma ändamål och medel för behandling av personuppgifter.

Brister i hanteringen kan medföra kränkning av den enskildes integritet och kan leda till både förtroendeskada och ekonomisk skada för SLU.

Vissa förändringar i regler kring skydd av den personliga integriteten har beslutats eller aviserats under 2015. Bland annat beslutade EU-kommissionen nya regler för att stärka skyddet av personuppgifter och därmed öka tryggheten för att lämna ut personuppgifter. De nya reglerna kommer att ersätta personuppgiftslagen 2018. Förändringarna har inte ingått i granskningen men aktualiserar vikten av att leva upp till nu gällande regler eftersom kraven kommer att skärpas under kommande år.

3 Granskningens omfattning och inriktning

Målet med granskningen är att bedöma om rutiner och processer för personuppgiftsbehandling följer gällande regelverk och är ändamålsenliga.

Internrevisionens bedömning utgår i huvudsak från personuppgiftslagen och från Datainspektionens skrifter. Då behandling av personuppgifter inte har granskats tidigare belyser granskningen främst hanteringen på övergripande nivå.

Granskningen har genomförts genom intervjuer och genomgång av regelverk och andra relevanta dokument. Internrevisionen har även tagit del av den arkivrevision¹ som juridik- och dokumentationsenheten genomförde 2014/2015 vid 50 enheter inom kärnverksamheten där personuppgifter var ett av de undersökta områdena. SLU:s personuppgiftsombud har intervjuats. Intervjuer har även gjorts med annan administrativ personal och forskare vid universitetsadministrationen, bibliotek och institutioner.

¹ Rapport efter arkivrevision inom SLU:s kärnverksamhet 2014/2015, SLU.ua.2015.2.1.1-2853.

4 Personuppgiftslag (1998:204)

Personuppgiftslagens syfte är att skydda människors personliga integritet mot kränkningar när personuppgifter behandlas. Lagen är subsidiär i förhållande till andra lagar, dvs. om det finns avvikande bestämmelser i annan lag eller förordning ska de bestämmelserna tillämpas.

Med personuppgifter avses all slags information som direkt eller indirekt kan kopplas till en viss person.² Med behandling menas allt man gör med personuppgifter. Exempel på behandling av personuppgifter är: insamling, registrering, bearbetning, lagring och spridning. I lagen ställs högre krav på behandling av uppgifter som är strukturerade t.ex. dataregister, databaser och ärende-/dokumenthanteringssystem.

För att få behandla personuppgifter i strukturerat material måste de grundläggande kraven i personuppgiftslagen vara uppfyllda, bl.a. att uppgifterna är lagliga, korrekta och enligt god sed. Dessutom ska den registrerade ge sitt samtycke. Det finns dock undantag då det är tillåtet att behandla personuppgifter utan samtycke. Det anges att personuppgifter får behandlas om det är nödvändigt för att kunna fullgöra ett avtal med den registrerade, en arbetsuppgift av allmänt intresse skall kunna utföras, myndighetsutövning eller efter intresseavvägning. Med intresseavvägning menas att personuppgifter får behandlas utan samtycke om personuppgiftsansvariges intresse av behandlingen väger tyngre än den registrerades intresse av skydd mot kränkningar av den personliga integriteten.

Innan behandling av personuppgifter påbörjas ska ändamålen med behandlingen bestämmas och antingen anmälas till Datainspektionen³ eller till personuppgiftsombudet om organisationen utsett sådan. Uppgifterna får inte behandlas för något annat ändamål än vad som bestämts när uppgifterna samlades in.

I personuppgiftslagen finns även regler för när personuppgifter får behandlas vid forskning. Känsliga personuppgifter får behandlas om behandlingen godkänts enligt etikprovningsslagen.

I personuppgiftslagen anges ett antal roller:

- *Personuppgiftsansvarig* är den juridiska person eller myndighet som bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Det är alltid personuppgiftsansvarig som har ansvaret gentemot de personer

² Exempel på personuppgifter är namn, adress, personnummer, telefonnummer, fastighetsförteckning, registreringsnummer på bil, kodade uppgifter om det existerar en kodnyckel, IP-nummer om det går att koppla till en viss person.

³ Datainspektionen är tillsynsmyndighet och ska bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet. Myndigheten utfärdar föreskrifter och allmänna råd samt ger ut informationsskrifter.

som är registrerade. Personuppgiftsansvaret är skadeståndssanktionerat och brott mot vissa regler är straffsanktionerat. Brott kan ge böter och fängelse.

- *Personuppgiftsombud* är den person som är utsedd av organisationen att se till att personuppgifter behandlas på ett korrekt och lagligt sätt och informera personuppgiftsansvarig om eventuella brister.
- *Personuppgiftsbiträde*, är någon utanför organisationen som fått personuppgiftsansvariges uppdrag att behandla personuppgifter. Biträdet får enbart behandla personuppgifter enligt de instruktioner och riktlinjer som personuppgiftsansvarig angett.

5 Interna styrdokument för personuppgiftsbehandling

Det saknas beskrivning över ansvar och befogenheter att behandla personuppgifter. Det saknas även tydliga anvisningar om hur behandling får utföras.

Personuppgiftslagen är ett generellt regelverk, dvs. den gäller inom alla typer av organisationer och sammanhang. Det kan därför vara svårt att bedöma hur lagen ska tillämpas inom just universitetets verksamheter, såväl inom grundutbildning och forskning som inom olika administrativa områden. Att lagen är subsidiär, dvs. att andra lagar och förordningar gäller framför personuppgiftslagen försvårar bedömningen ytterligare.

I delegationsordning för universitetsadministrationen⁴ anges att chefsjuristen är personuppgiftsombud för SLU. I övrigt saknar det interna regelverket beskrivning av hur och till vem ansvar och befogenheter att behandla personuppgifter har delegerats. Detta gäller både personuppgiftslagen och etikprovningsslagen.

På SLU:s hemsida finns information om personuppgiftslagen och etikprovning med länkar till Datainspektionen och Etikprovningssnämnden⁵ samt kontaktuppgifter till personuppgiftsombudet. Det finns information om rätten att begära ut information om de personuppgifter som finns registrerade på SLU. Dock saknas information om möjligheten att få rättelse om uppgifterna är felaktiga. Utöver den information som finns på hemsidan saknas anvisningar för hur personuppgifter ska behandlas inom universitetet.

Det finns policyer och riktlinjer för säkerhet inom SLU som även rör IT och informationssäkerhet. Dessa berör i viss mån personuppgifter i samband med informationssäkerhetsklassning. Det finns även tips och råd om hur man ska

⁴ Organisation och ansvarsfördelning inom universitetsadministrationen, Dnr SLU ua 2014.1.1.1-1030

⁵ Etikprovningssnämnderna, en central och sex regionala, utövar etikprovning som fristående myndigheter.

skydda information på dator, smartphone, surfplatta och externa lagringsenheter samt en flödesbeskrivning för lagring i molnet.

Den snabba tekniska utvecklingen ger allt större möjligheter att lagra och överföra information på olika sätt. Samtidigt ökar risken för integritetskränkningar likväl som medvetenheten om den personliga integriteten ökar hos allmänheten. Internrevisionen anser att det utöver de tips och råd som anges ovan bör finnas tydliga anvisningar vid personuppgiftsbehandling angående vad som är tillåtet när det gäller lagring och överföring av personuppgifter i såväl universitetsägd som privat utrustning.

Brister i regelverket har även påtalats i juridik- och dokumentationsenhetens arkivrevision. I rapporten föreslås att en policy och riktlinjer för informationshantering tas fram för att samla alla aspekter på informationshantering: informationssäkerhet, personuppgiftsbehandling och hantering av verksamhetens informationstillgångar. Internrevisionen delar i enlighet med rapportens bedömning att det vore en fördel med ett enhetligt regelverk för informationshantering, oavsett om informationen finns rent fysisk eller bara digitalt och oavsett olika tekniska lösningar.

A. Internrevisionen rekommenderar att universitetsledningen säkerställer att ansvar och befogenheter för behandling av personuppgifter, enligt såväl personuppgiftslagen som etikprövningslagen, finns beskrivet i det interna regelverket.

B. Internrevisionen rekommenderar att universitetsledningen säkerställer att instruktioner om hur personuppgifter får behandlas inom SLU finns tydligt beskrivet.

C. Internrevisionen rekommenderar att universitetsledningen säkerställer att det finns lättillgänglig information för medarbetare, studenter och allmänheten om möjligheten att få rättelse om registrerade uppgifter är felaktiga.

D. Internrevisionen rekommenderar att universitetsledningen överväger att utforma ett gemensamt regelverk för informationshantering enligt juridik- och dokumentationsenhetens förslag.

6 Hantering av personuppgifter inom SLU

6.1 Personuppgiftsombudets uppgift

SLU:s personuppgiftsombud utför inte samtliga uppgifter som åligger funktionen enligt personuppgiftslagen.

Enligt personuppgiftslagen ska personuppgiftsombudet självständigt se till att personuppgifter behandlas på ett korrekt och lagligt sätt. Ombudet ska;

- utöva tillsyn över behandlingar och anmäla brister,
- samråda med Datainspektionen vid tveksamheter om lagens tillämpning,
- föra förteckning över behandlingar och
- hjälpa registrerade att få rättelse.

Förutom det som anges i lagen har Datainspektionen tagit fram en informationsbroschyr riktad till personuppgiftsombudet som stöd för hur de ska utföra sina uppgifter. För att kunna kontrollera att personuppgifter behandlas på ett lagligt och korrekt sätt föreslås bl.a. att personuppgiftsombudet utarbetar rutiner för sin kontrolluppgift.

Chefsjuristen är utsedd till personuppgiftsombud för SLU men har möjlighet att delegera uppgiften. Uppgiften att föra förteckning över behandlingar har delegerats till annan jurist, men delegationen har ännu inte formaliserats.

Personuppgiftsombudet tar emot anmälningar och förtecknar de behandlingar som anmälts. Internrevisionen har tagit del av förteckningar över anmälningar. De stickprov som togs på anmälningar visar att de i huvudsak innehåller de uppgifter som krävs. Det är enligt ombudet troligt att det finns behandlingar som inte har anmälts till personuppgiftsombudet.

Endast ett fåtal av de intervjuade vet att SLU har ett personuppgiftsombud, dennes uppgift och placering inom organisationen. Även kravet på att anmäla behandling av personuppgifter är okänt. Kunskapen om vad behandling av personuppgifter omfattar varierar. Det finns däremot en tydlig medvetenhet om att personnummer ska hanteras försiktigt. De intervjuade personer som dagligen arbetar med personuppgifter har god kunskap inom sina områden.

Det sker i stort sett ingen tillsyn av hur personuppgifter behandlas inom SLU. Personuppgiftsombudet är väl medveten om att det finns brister när det gäller tillsynen. I den informationssäkerhetsklassning som Infra har påbörjat finns en viss kontroll av personuppgiftsbehandling. Även juridik- och dokumentationsenhetens arkivrevision 2014-2015 kan ses som en kontrollaktivitet. Dock är inte personuppgiftsombudet involverad i dessa aktiviteter.

Personuppgiftsansvarig, dvs. SLU, har skyldighet enligt lag att rätta, blockera eller utplåna missvisande eller felaktiga uppgifter om den registrerade begär detta. Personuppgiftsombudet har inte fått in någon begäran om rättelse. Datainspektionen föreslår att det finns rutiner för denna hantering och att ombudets roll beskrivs tydligt för både registrerade och för medarbetare i organisationen.

Personuppgiftsansvarig har även i uppgift att på begäran från registrerad lämna ut de uppgifter som finns registrerat om personen.⁶ Det har inkommit ett fåtal sådana ansökningar. Uppgifter har då sökts fram från de största och mest bekanta administrativa systemen. Det saknas rutiner för att med säkerhet kunna lämna fullständiga uppgifter till den registrerade.

E. Internrevisionen rekommenderar att universitetsledningen säkerställer att personuppgiftsombudets uppgifter utförs enligt personuppgiftslagen.

6.2 Personuppgiftsbehandling utanför SLU

Det finns risk att personuppgiftsbehandling överläts till extern leverantör utan att SLU:s instruktioner och villkor finns angivet i personuppgiftsbiträdesavtal. Detta kan leda till att personuppgifterna inte behandlas enligt personuppgiftslagen och det interna regelverket.

Allt fler myndigheter, kommuner och företag använder sig av så kallade molntjänster. Personuppgifter som hanteras av molntjänstleverantörer kan överföras till tredje land. Detta kunde tidigare ske med stöd av regler om personlig integritet och dataskydd som USA tagit fram för organisationer i USA, de s.k. Safe Harbour-principerna. EU bedömde tidigare att det var en lämplig skyddsnivå för överföring till USA. Dock ogiltigförklarades Safe harbour-principerna i en dom i EU-domstolen i oktober 2015. Domen bedöms få konsekvenser för molntjänstleverantörer och därmed även för de som köper deras tjänster.

SLU har alltid ansvaret för att personuppgiftslagen följs men kan överlåta den faktiska behandlingen till extern leverantör, exempelvis via molntjänst. Universitetet ska då teckna ett s.k. personuppgiftsbiträdesavtal med leverantören. Det finns inget krav att avtalen ska upprättas i samråd med jurist.

Internrevisionen anser det viktigt att personuppgiftsbiträdesavtal utformas så att SLU:s krav för personuppgiftsbehandling tydligt framgår. Vid upprättande av avtal är det viktigt att säkerställa att personuppgifter inte överförs till tredje land utan en godkänd skyddsnivå. Ju känsligare uppgifter som behandlas, desto högre är kravet på att personuppgiftsansvarig ska ha möjligheter att kontrollera att biträdena följer lagen och de angivna instruktionerna.

⁶ Den registrerade har enligt personuppgiftslagen rätt att en gång per kalenderår gratis få besked om vilka personuppgifter som finns om hen hos den personuppgiftsansvariga organisationen.

F. Internrevisionen rekommenderar att universitetsledningen säkerställer att personuppgiftsbiträdesavtal alltid upprättas i samråd med juristerna för att säkerställa SLU:s ansvar.

6.3 Personuppgiftsbehandling i forskning

Det finns risk att det inom SLU bedrivs forskning på människor som inte hanteras enligt personuppgifts- och etiklagstiftningen. Förutom att tillståndspliktig forskning utan etikprövningstillstånd är att betrakta som oredlighet i forskning, kan det även leda till att forskningsresultat inte publiceras. Det kan givetvis också skada universitetets anseende.

En av de situationer då behandling av personuppgifter är av allmänt intresse enligt personuppgiftslagen är forskning. Forskning som rör känsliga⁷ personuppgifter får endast behandlas om forskningsändamålet godkänts av Etikprövningsnämnden innan forskningen påbörjats. Forskningsprojekt som fått godkännande ska även anmäla behandlingen till personuppgiftsombudet.

Forskningsprojekt som omfattar personuppgifter är inte vanligt förekommande inom SLU. Under perioden 2014-sept 2015 lämnade universitetet in sex ansökningar till Etikprövningsnämnden. Internrevisionen har tagit del av fyra av dessa ansökningar och intervjuat ansvariga forskare (två stycken). Ett av projekten anmäldes till personuppgiftsombudet sedan ombudet fått vetskap om projektet. Två projekt anmäldes i samband med internrevisionens granskning. Att ingen anmälan gjorts tidigare berodde på att momentet inte var känt för forskarna. Forskarna uppgav också att de haft stöd vid etikprövning av mer erfarna kollegor från andra lärosäten.

I de kurser som ges till forskare om försöksdjurshandling nämns personuppgiftslagen. Enligt SLU:s försöksdjurskoordinator förekommer forskning på privatägda djur där ägarnas personuppgifter behandlas. Det kan även förekomma att prover tas på djurägare. Koordinatören upplever att det finns behov av mer utförlig information vid dessa kurser för att minska risken för felaktig hantering av personuppgifter. Det kan även finnas risk för att forskning sker utan tillstånd från etikprövningsnämnden men den risken är väsentligen mindre.

Personuppgiftsombudet känner viss oro över att personuppgifter inom forskning inte hanteras korrekt. Risken ökar i och med att forskning på människor är relativt ovanligt inom SLU och därmed saknas ofta kännedom om vilka regler som gäller. Samtidigt närmar sig forskningen i flera fall humanområdet, alltmer forskning är gränsöverskridande och teknikutveckling möjliggör användande av personuppgifter i forskning på ett annat sätt.

⁷ Känsliga personuppgifter är sådana uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv. Uppgifter om hälsa kan vara till exempel sjukfrånvaro, graviditet och läkarbesök.

Internrevisionen anser att behandling av personuppgifter, främst känsliga uppgifter, i forskning är en viktig fråga. Felaktig behandling kan utöver kränkning av den personliga integriteten skada både det enskilda forskningsprojektet och SLU:s anseende. Om forskning inte har ett godkännande av etikprövningsnämnden finns risk att den inte kan publiceras då vetenskapliga tidskrifter ofta kräver att studien etikprövats. Skulle forskningen ändå publiceras gör forskaren sig skyldig till oredlighet i forskning.

G. Internrevisionen rekommenderar att universitetsledningen säkerställer att doktorander och forskare får relevant information om hur de ska hantera personuppgifter i forskningsprojekt i enlighet med personuppgiftslagen och etikprövningslagen.

Inga Astorsdotter

Lisbeth Sundkvist Johansson

Internrevisionschef

Internrevisor

Bilaga 1. Regler som berör personuppgifter och säkerhet.

Externa regelverk

- Tryckfrihetsförordning (1949:105)
- Offentlighets- och sekretesslag (2009:400)
- Förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor
- Personuppgiftslag (1998:204)
- Personuppgiftsförordning (1998:1191)
- Lag (2003:460) om etikprövning av forskning som avser människor
- Förordning (2003:615) om etikprövning av forskning som avser människor
- Lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa
- Lag (2003:389) om elektronisk kommunikation
- Myndighetsförordning (2007:515)
- Förvaltningslag (1986:223)
- Datainspektionens myndighetsföreskrifter

Interna styrdokument som avser säkerhet inom SLU:

- Säkerhetspolicy för SLU, Dnr SLU ua 2014.2.10-1367
- It-policy vid SLU, fastställd av rektor 2005-08-29
- It-säkerhetspolicy finns på medarbetarwebben.
- Riktlinjer för informationssäkerhet vid SLU, Dnr SLU ua 2015.2.10-2118
- Riktlinjer för informationssäkerhetsklassning, DNR SLU ua 2015.2.10-2115

Åtgärdsplan med anledning av internrevisionens rapport avseende Personuppgiftslagen

Internrevisionen konstaterar i sin rapport Personuppgiftslagen att det finns brister i hanteringen av personuppgifter vid SLU. Med anledning av detta rekommenderar internrevisionen ett antal olika åtgärder.

De väsentliga rekommendationerna är följande:

1. att ansvar och befogenheter för behandling av personuppgifter, enligt såväl personuppgiftslagen som etikprovninglagen, finns beskrivet i det interna regelverket,
2. att instruktioner om hur personuppgifter får behandlas inom SLU finns tydligt beskrivet och
3. att personuppgiftsombudets uppgifter utförs i enlighet med personuppgiftslagen.

Alla internrevisionens rekommendationer redovisas nedan kompletterade med kommentarer och förslag till åtgärder.

Interna styrdokument för personuppgiftsbehandling

Internrevisionen rekommenderar att universitetsledningen:

A säkerställer att ansvar och befogenheter för behandling av personuppgifter, enligt såväl personuppgiftslagen som etikprovninglagen, finns beskrivet i det interna regelverket.

B säkerställer att instruktioner om hur personuppgifter får behandlas inom SLU finns tydligt beskrivet.

C säkerställer att det finns lättillgänglig information för medarbetare, studenter och allmänheten om möjligheten att få rättelse om registrerade uppgifter är felaktiga.

D överväger att utforma ett gemensamt regelverk för informationshantering enligt juridik- och dokumentationsenhetens förslag.

Kommentarer:

Personuppgifter och hur de ska behandlas regleras i svensk lag. Något internt regelverk behövs av den anledningen inte, men det är viktigt att de regler som gäller tydliggörs och att SLU har anvisningar för hanteringen av personuppgifter.

Åtgärder:

A och B Nya anvisningar och text som tydliggör regelverket arbetas fram och läggs ut på SLU:s hemsida. Överväga ny organisation för hur personuppgiftsombudets uppgifter utförs.

Ansvar: Ledningskansliet. Klart: 2017-05-31. Dok: Medarbetarwebb

C Detta kommer att anges som information på SLU:s hemsida.

Ansvar: Ledningskansliet. Klart: 2017-03-31. Dok: Medarbetarwebb

D Arbete med detta finns redan inplanerat i Ledningskansliets verksamhetsplan för 2016.

Ansvar: Ledningskansliet. Klart: 2017-03-31. Dok: Medarbetarwebb

Hantering av personuppgifter inom SLU

Internrevisionen rekommenderar att universitetsledningen:

E säkerställer att personuppgiftsombudets uppgifter utförs enligt personuppgiftslagen.

F säkerställer att personuppgiftsbiträdesavtal alltid upprättas i samråd med juristerna för att säkerställa SLU:s ansvar.

G säkerställer att doktorander och forskare får relevant information om hur de ska hantera personuppgifter i forskningsprojekt i enlighet med personuppgiftslagen och etikprövningslagen.

Kommentarer:

SLU eftersträvar att personuppgiftsbiträdesavtal upprättas i samråd med juristerna. Varken IT-avdelningen eller någon annan del av universitetsadministrationen får kännedom om alla it-samarbeten vid SLU. Ledningen bedömer att förtydligande information är det sätt SLU kan arbeta på för att försöka säkerställa att juristerna får möjlighet att vara med när personuppgiftsbiträdesavtal upprättas.

Åtgärder:

E Undersöka möjligheten att omorganisera personuppgiftsombudets roll och delegera ansvaret till fler personer.

Ansvar: Universitetsdirektören. Klart: 2017-05-31.

Dok: Universitetsdirektörsbeslut

F Ingen åtgärd utöver informations- och utbildningsinsatser.

G Regelverket förtydligas genom information på hemsidan samt genom introduktionsutbildning för doktorander och information till dem som söker forskningsmedel.

Ansvar: Ledningskansliet. Klart: 2017-03-31. Dok: Medarbetarwebb
