Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

**Styrelsen**

**BESLUT**

SLU ID: SLU ua 2021.1.1.2-388

2021-09-28

Rektor

# Hantering av dataskyddsförordningen

## Beslut

Styrelsen beslutar

att lägga internrevisionens rapport *Hantering av dataskyddsförordningen* till handlingarna, samt

att fastställa rektors åtgärdsplan med anledning av rapporten.

## Ärendet

Internrevisionen har i enlighet med revisionsplanen för 2021 granskat SLU:s hantering av dataskyddsförordningen. Syftet med granskningen har varit att bedöma om SLU:s processer och rutiner för hantering av personuppgifter är ändamålsenliga och i enlighet med dataskyddsregelverket.

Internrevisionens sammanfattande bedömning är att det finns brister i hanteringen av dataskyddsförordningen (GDPR). Detta kan leda till att övervakning inte sker enligt GDPR samt att SLU inte efterlever förordningen med risk för sanktioner och försämrat anseende. Med anledning av detta har ett antal rekommendationer lämnats. Av rektors åtgärdsplan framgår vilka åtgärder som ledningen bedömer bör vidtas.

Beslut i detta ärende har fattats av styrelsen efter föredragning av internrevisor Lisbeth Sundkvist Johansson. Åtgärdsplanen har beretts av universitetsdirektör Martin Melkersson och Miika Wallin, chef för ledningskansliet. Åtgärdsplanen har föredragits av universitetsdirektör Martin Melkersson.

Rolf Brennerfelt

Lisbeth Sundkvist Johansson

Postadress: Box 7070 75007 Uppsala
Besöksadress: Almas alle´8
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)
Lisbeth.sundkvist.johansson@slu.se

Kopia för kännedom

Prorektor
Dekanerna
Avdelningschefer (motsv.) inom universitetsadministrationen
Universitetdjursjukhusdirektör
Överbibliotekarie
SLUSS

Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

**Internrevision**

**RAPPORT**

SLU ID: SLU.ua 2021.1.1.2-388

2021-08-30

# Hantering av dataskyddsförordningen

Rapport från internrevisionen

Postadress: Box 7086
Besöksadress: Almas allé 8
Org nr: 202100-2817
www.slu.se

Tel: 018-67 10 00 (vx)

Lisbeth.sundkvist.johansson@slu.se

# Innehåll

1. Sammanfattning ..... 3

2. Bakgrund och motiv ..... 4

3. Syfte och mål ..... 4
   3.1 Omfattning, avgränsningar och metod ..... 4

4. Hantering av dataskyddsförordningen ..... 5
   4.1 Styrdokument ..... 5
   4.2 Organisation och ansvar ..... 6
   4.3 Övervakning och återrapportering av hur GDPR efterlevs ..... 8
   4.4 Konsekvensbedömningar avseende dataskydd ..... 8
   4.5 Personuppgiftsincidenter ..... 9
   4.6 Register över personuppgiftsbehandlingar ..... 9
   4.7 Överföring av uppgifter till tredje land ..... 10

5. Analys och bedömning ..... 11

6. Rekommendationer ..... 12

# 1. Sammanfattning

Internrevisionen har i enlighet med revisionsplanen för 2021 granskat SLU:s hantering av dataskyddsförordningen. Syftet med granskningen har varit att bedöma om SLU:s processer och rutiner för hantering av personuppgifter är ändamålsenliga och i enlighet med dataskyddsregelverket.

Internrevisionens sammanfattande bedömning är att det finns brister i hanteringen av dataskyddsförordningen (GDPR). Detta kan leda till att övervakning inte sker enligt GDPR samt att SLU inte efterlever förordningen med risk för sanktioner och försämrat anseende.

Internrevisionens bedömning grundar sig i huvudsak på följande:

- Att SLU:s ansvar i egenskap av personuppgiftsansvarig inte särskiljs från dataskyddsombudets ansvar att övervaka efterlevnaden.
- Att dataskyddsfunktionens resurser omfattar både personuppgiftsansvarigs och dataskyddsombudets ansvarsområden vilket försvårar möjligheten att särskilja ombudets resursbehov i form av kompetens, stödresurser och tid.
- Att de övervakningsinsatser som genomförts utöver informationsinsatser har varit begränsade. Utan tydlig metod för övervakningsarbetet samt systematiska uppföljningsrutiner och god dokumentation är det svårt att bedöma hur väl SLU efterlever GDPR.
- Att det inte finns någon formell rutin för hur brister som dataskyddsombudet påtalar ska hanteras. Detta riskerar leda till att noterade brister kvarstår.
- Att det finns brister i information och vägledning för konsekvensbedömningar avseende dataskydd.
- Att det saknas formell rutin för hantering av registerförfrågningar vilket kan leda till att felaktig information lämnas ut eller att personuppgifter hanteras felaktigt.

Rekommendationerna i rapporten är i korthet följande:

- Att regelverket om dataskyddsförvaltning uppdateras så att gränsdragningen blir tydlig mellan verksamhetens ansvar att säkerställa att SLU som personuppgiftsansvarig följer GDPR och dataskyddsombudets ansvar att övervaka efterlevnaden.
- Att det finns tillräckliga resurser i form av kompetens, stödresurser och tid för dataskyddsombudet i enlighet med GDPR.
- Att dataskyddsombudets metod för övervakningsarbete, uppföljning och dokumentation förbättras för att öka kvaliteten i övervakning av SLU:s följsamhet mot GDPR.
- Att rutiner formaliseras för hur de brister som dataskyddsombudet rapporterar till styrelsen ska hanteras.
- Att verksamheten informeras om att konsekvensbedömningar avseende dataskydd ska genomföras.
- Att rutiner för hantering av registerförfrågningar formaliseras.

# 2. Bakgrund och motiv

Dataskyddsförordningen (GDPR) är till för att skydda enskildas grundläggande fri- och rättigheter, särskilt rätten till skydd av personuppgifter. Förordningen har bland annat till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter. Detta innebär att samtliga verksamheter inom EU som hanterar personuppgifter ska göra det utifrån GDPR. Utöver GDPR har Sverige den kompletterande dataskyddslagen (2018:218) som medger vissa undantag och anpassningar till svensk rätt, exempelvis att myndigheter kan tvingas betala sanktionsavgifter om de bryter mot förordningen. Förutom dataskyddslagen finns s.k. registerförfattningar som reglerar hur personuppgifter får hanteras i vissa offentliga verksamheter, exempelvis patientdatalagen och studiestödsdatalagen. Eftersom dataskyddslagen är subsidiär har registerförfattningarna företräde framför dataskyddslagen, men måste ändå stämma överens med GDPR.

Integritetsskyddsmyndigheten (IMY) är Sveriges tillsynsmyndighet för behandling av personuppgifter. De har i uppdrag att granska att reglerna inom dataskyddsområdet följs. Under 2020 beslutade IMY om sanktionsavgifter på 150 miljoner kronor, i huvudsak mot olika verksamheter som inte har följt GDPR.[1] En av dessa är Umeå universitet som hanterade känsliga personuppgifter felaktigt vilket resulterade i en sanktionsavgift på 550 tkr.

Internrevisionen granskade 2015 rutiner och processer för behandling av personuppgifter utifrån då gällande regelverk och inför införandet av GDPR 2018. Granskningen visade på brister gällande ansvar, instruktioner och tillsyn. SLU inledde därefter ett omfattande arbete med anpassning till de nya reglerna för personuppgiftshantering och har vidtagit ett antal åtgärder för att förbättra situationen. Vissa indikatorer tyder dock på att regelefterlevnaden av GDPR är ojämn och att brister kvarstår. Detta kan skada universitetets anseende och leda till sanktioner.

# 3. Syfte och mål

Syftet med granskningen har varit att bedöma om SLU:s processer och rutiner för hantering av personuppgifter är ändamålsenlig och i enlighet med dataskyddsregelverket.

## 3.1 Omfattning, avgränsningar och metod

Granskningen har genomförts via intervjuer och dokumentstudier. Granskningens grunder för bedömning har utgått från de krav som ställs i GDPR och tillhörande EU-gemensamma riktlinjer. Granskningens fokus har varit organisation, ansvar och roller för dataskyddsombud.

[1] IMY 2021-02-22

Dataskyddsarbetet är nära sammanlänkat med informationssäkerhetsarbetet. Till stor del handlar säkerhetsarbetet om att hantera och minimera risker. Internrevisionen avser att göra en separat granskning av informationssäkerhet under hösten 2021 som även kommer att omfatta molntjänster.

# 4. Hantering av dataskyddsförordningen

**Det finns brister i ansvarsfördelningen mellan SLU som personuppgiftsansvarig och dataskyddsombudet vilket kan innebära att dataskyddsombudets uppgifter inte särskiljs från SLU:s ansvar. Detta kan leda till att övervakning inte sker enligt GDPR samt att SLU inte efterlever förordningen vilket kan skada universitetets anseende och leda till sanktioner.**

## 4.1 Styrdokument

Alla verksamheter som hanterar personuppgifter måste följa GDPR. I förordningen beskrivs ett antal roller med olika ansvar, till exempel personuppgiftsansvarig och dataskyddsombud.

Personuppgiftsansvarig är den organisation som ansvarar för personuppgifterna och bestämmer för vilka ändamål behandlingen görs och hur det ska gå till. Personuppgiftsansvarig ska därmed genomföra lämpliga åtgärder, såväl tekniska som organisatoriska, för att säkerställa och visa att personuppgiftsbehandling utförs enligt GDPR. Enligt IMY kan personuppgiftsansvarig visa att de uppfyller förordningens bestämmelser genom exempelvis en policy för dataskydd som beskriver hur dataskyddsarbetet genomförs i organisationen.

Dataskyddsombud är en roll som enligt GDPR ska utses av personuppgiftsansvarig för att bland annat övervaka att förordningen efterlevs.

Det finns ett antal beslut om SLU:s hantering av personuppgifter; beslut om dataskyddsombud[2], dataskyddsförvaltning[3] samt rutiner för personuppgiftsbehandling inom forskningsprojekt[4]. Ledningskansliet har ansvar för att stödja SLU:s hantering av personuppgifter.

Utöver dessa beslut har ett flertal dokument tagits fram och tillgängliggjorts på SLU:s hemsidor. Bland annat finns två dataskyddshandböcker varav en är särskilt riktad till de som handleder studentarbeten. Det finns även snabbguider, rekommendationer samt olika mallar och blanketter. På webbsidorna anges kontaktvägar till dataskyddsombudet. Handböckerna beskriver hur personuppgifter får användas inom SLU och vad som krävs för att få behandla personuppgifter.

[2] Rektorsbeslut. Personuppgiftsombud och Dataskyddsombud vid SLU, SLU.ua.2017.1.1.1-2300.
[3] Universitetsdirektörsbeslut. Dataskyddsförvaltning vid SLU, SLU.ua 2018.1.1.1-1922.
[4] Universitetsdirektörsbeslut. Rutiner för att dokumentera personuppgiftsbehandling inom forskningsprojekt i enlighet med dataskyddsförordningen, SLU.ua 2018.1.1.1-1921.

Handböckerna är dock inte tillgängliga i sin helhet utan är uppdelade i avsnitt vilket försvårar sökbarheten.

Det finns information till registrerade, såväl studenter som anställda, om hur personuppgifter hanteras inom SLU. Informationen finns tillgänglig på Studentwebben och Medarbetarwebben. Information om hur personuppgifter behandlas finns i ett antal system, exempelvis i e-postsystemet och i rekryteringsverktyget ReachMee.

## 4.2 Organisation och ansvar

SLU måste som personuppgiftsansvarig se till att behandlingen av personuppgifter sker i enlighet med bestämmelser i GDPR. I ansvaret ligger även att visa att behandlingen utförs enlig förordningen.

Personuppgiftsansvarig ska utse dataskyddsombud. Denne ska utses på grundval av yrkesmässiga kvalifikationer, sakkunskap om dataskyddslagstiftning och praxis samt förmågan att fullgöra de uppgifter som anges i förordningen. Som personuppgiftsansvarig har även SLU ansvar att se till att ombudet har rätt förutsättningar för att utföra sina uppgifter, exempelvis tillräckligt med tid, tillgång till nödvändig information samt vidareutbildning. IMY anger utöver det olika exempel på personuppgiftsansvarigs ansvar mot dataskyddsombudet.

SLU har sedan 2018 ett utsett dataskyddsombud. Ansvar för att SLU behandlar personuppgifter enligt GDPR ligger på den s.k. dataskyddsfunktionen som skapades utifrån beslut om dataskyddsförvaltning[5]. Funktionen utgörs av två universitetsjurister, varav en har uppdraget som dataskyddsombud. Funktionen ska bestå av 1,5 HÅA. I beslutet anges funktionens ansvar för övervakning, löpande arbete, stöd till verksamheten och ansvar för interna styrdokument. Dock är uppgifterna sammanblandande och det framgår inte vad som är dataskyddsombudets ansvarsområde och vad som avser den personuppgiftsansvariges ansvarsområde. Funktionen ska enligt beslutet utöver juristerna ha tillgång till ett nätverk med annan kompetens som behövs. I övrigt följer ansvar för att följa GDPR samma chefslinje som övrig regelefterlevnad.

Ett nätverk inrättades 2018 till stöd för dataskyddsfunktionen där bland annat informationssäkerhetsstrategen och representant från it-avdelningen ingick. Funktionen och nätverket hade från start regelbundna möten för att helt upphöra vid årsskiftet 2019/2020. Två av tjänsterna, en jurist samt SLU:s informationssäkerhetsstrateg, har varit vakanta från årsskiftet 2020/2021.

[5] Beslut av universitetsdirektörsbeslut om dataskyddsförvaltning SLU ua 2018.1.1.1-1922.

*Dataskyddsombudets ansvar*

Dataskyddsombudet ansvarar inte för att SLU följer GDPR. Det ansvaret ligger alltid hos personuppgiftsansvarig. Dataskyddsombudet ska kunna arbeta självständigt och oberoende och utan påverkan från andra inom organisationen. Det är viktigt att personens övriga arbetsuppgifter inom organisationen inte krockar med rollen som dataskyddsombud. Det är exempelvis olämpligt att hen har en ledningsroll och/eller deltar i strategiska beslut rörande personuppgiftsbehandling.

Dataskyddsombudets viktigaste uppgift är att övervaka att organisationen följer GDPR. Detta kan ske genom att

- samla in information för att identifiera hur behandling av personuppgifter sker,
- analysera och kontrollera hur GDPR och interna bestämmelser om behandlingen efterlevs,
- informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige.[6]

Rollen ska dessutom ge råd om konsekvensbedömningar avseende dataskydd, vara kontaktperson mot IMY, anställda inom organisationen och registrerade personer samt samarbeta med IMY vid exempelvis inspektioner.

SLU:s dataskyddsombud är heltidsanställd universitetsjurist.[7] Utöver att det i ovan angivna beslut angetts att förvaltningsfunktionen ska bestå av 1,5 HÅA finns inget specifikt angivet om hur stor del av ombudets arbetstid som avser ombudsrollen.

Vid intervju med dataskyddsombudet framgår att personen inte anser sig ha den kompetens som krävs för rollen och att merparten av arbetet har utförts av funktionens andra jurist. Enligt ombudet har det, efter att denne slutat, inte funnits vare sig tid eller kompetens för uppdraget då andra arbetsuppgifter prioriteras. Detta har ombudet rapporterat till styrelsen i juni 2021. En uppfattning som framkommit under granskningen är att momenten kontroll och information som ingår i dataskyddsombudets uppdrag inte kan genomföras av enbart en person då det innebär konflikt med rollens självständighet och oberoende.

Enligt uppgift pågår diskussioner om hur dataskyddsfunktionen ska utformas samt var dataskyddsombudet ska ha sin organisatoriska placering. Det finns enligt GDPR inget hinder mot att en grupp personer utför dataskyddsombudets uppgifter så länge alla i gruppen uppfyller de krav som ställs på dataskyddsombudet och att det framgår att arbetet sker under det utsedda dataskyddsombudets ansvar. IMY rekommenderar att organisationen dokumenterar uppgiftsfördelningen mellan de

[6] Riktlinjer om dataskyddsombud, Artikel 29-arbetsgruppen för skydd av personuppgifter. Arbetsgruppen är ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet.
[7] Rektorsbeslut SLU.ua.2017.1.1.1-2300 som omfattade beslut om både personuppgiftsombud och dataskyddsombud.

personer som utför dataskyddsombudets uppgifter. Andra alternativ som IMY anger är att anlita en extern konsult som dataskyddsombud eller att dela rollen med annan myndighet.

## 4.3 Övervakning och återrapportering av hur GDPR efterlevs

Dataskyddsfunktionen har som en del av dataskyddsombudets övervakningsuppdrag genomfört informations- och utbildningsinsatser under åren 2018-2020. Utbildningsinsatser har genomförts vid introduktionsdagar, chefsutbildning, prefektdagar och doktorandutbildning. Det har även genomförts riktade informationsinsatser mot institutioner, centrala avdelningar samt till enskilda forskare. Under granskningen har det framförts att dataskyddsfunktionens informationsinsatser varit värdefulla i arbetet med dataskydd.

För att kontrollera hur reglerna följs har funktionen genomfört två enkäter. Under 2019 riktades en enkät till prefekter om följsamhet mot beslut om rutiner för dataskyddshantering vid forskning med svar från 23 institutioner. Våren 2020 skickades en enkät om efterlevnad till prefekter, dekaner, fakultetsdirektörer samt avdelningschefer med svar från 14 chefer vilket ger en svarsfrekvens på 25 %, vilket är mycket lågt för att bedöma efterlevnad av GDPR. Vilka kontroller som genomförts i övrigt för att bedöma efterlevnad har inte dokumenterats.

Enligt GDPR ska dataskyddsombudet rapportera direkt till den högsta förvaltningsnivån, d.v.s. styrelsen. Rapporteringen är en del av dataskyddsombudets uppdrag att ge information och råd till personuppgiftsansvarig. Ett exempel på rapportering är att dataskyddsombudet utarbetar en årsrapport om sin verksamhet som lämnas till styrelsen.

Styrelsen har vid tre tillfällen, juni 2019, 2020 och 2021 tagit del av rapportering om SLU:s skydd för personuppgifter. Rapporterna omfattar beskrivning av arbete inom dataskyddsfunktionen, personuppgiftsincidenter, registrerade behandlingar, informationsinsatser, bedömning av brist- och riskområden inom regelefterlevnad där det finns behov av åtgärder. Det framgår dock i rapporten 2020 att det inte är dataskyddombudets rapport utan en rapport från den andra universitetsjuristen i funktionen. Årsrapporten för 2021 belyser flera områden av de områden som internrevisionens noterat, bland annat utformningen av dataskyddsfunktionen.

Det finns inga formella rutiner för hur ledningen ska hantera och bemöta de brister som rapporteras till styrelsen. Vid rapporteringen 2021 lämnade universitetsdirektören emellertid en kommentar till årsrapporten. Detta ser internrevisionen som en god rutin som bör formaliseras.

## 4.4 Konsekvensbedömningar avseende dataskydd

Konsekvensbedömning avseende dataskydd är ett verktyg för att skapa och påvisa efterlevnad av GDPR. En konsekvensbedömning ska genomföras om en planerad behandling av personuppgifter sannolikt leder till höga risker för de registrerades

fri- och rättigheter. Konsekvensbedömningen syftar till att belysa och hantera dessa risker. I bedömningen ingår att då ta fram rutiner och åtgärder för att möta dessa risker samt visa att man uppfyller kraven i GDPR.

Det är SLU:s ansvar att se till att konsekvensbedömningar avseende dataskydd sker. Dataskyddsombudet ska tillfrågas för råd vid dessa bedömningar. Funktionen har endast vid ett fåtal tillfällen blivit kontaktad angående råd vid konsekvensbedömning. Dessa fall har rört forskningsprojekt. Funktionen har i rapport till styrelsen 2020 lyft risker kring användandet av felaktigt behandlade personuppgifter vid forskning och att det i värsta fall kan leda till konsekvenser som forskningsetiska brister, oredlighetsärenden, utebliven finansiering eller alternativt återkrav av beviljad finansiering. Bristande personuppgiftsbehandling i forskningsprojekt kan enligt uppgift innebära att IMY kan bedöma att forskningsprojekt ska upphöra.

Konsekvensbedömning avseende dataskydd nämns kort i dataskyddshandböckerna under avsnitt om säkerhet. Det framgår dock inte vikten av att sådan bedömning görs vid personuppgiftsbehandling. Informationen är inte lättillgänglig då den inte går att nå via sökfunktionen på medarbetarwebben. Den mall för bedömning som finns framtagen, är inte tillgänglig för nedladdning utan lämnas ut vid förfrågan av dataskyddsombudet.

## 4.5 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors fri- och rättigheter. Personuppgiftsansvarig måste hantera personuppgiftsincidenter enligt de rutiner som förskrivs i GDPR. Vissa typer av personuppgiftsincidenter ska anmälas till IMY inom 72 timmar om de kan leda till risk för personers fri- och rättigheter.

SLU har ett IA-system[8] ”När något hänt” där personuppgiftsincident nämns som exempel på incidenter som kan anmälas. I övrigt saknas information om hur man ska agera vid misstanke om personuppgiftsincidenter. Dataskyddsombudet har sedan införandet av GDPR fått in ett fåtal anmälningar om personuppgiftsincidenter, och har i ett antal fall rapporterat dessa till IMY. Dataskyddsombudet har ingen helhetsbild men anser att det troligen är en underrapportering. Liksom vid konsekvensbedömningar är fallen få.

## 4.6 Register över personuppgiftsbehandlingar

SLU är skyldig att föra register över behandlingar av personuppgifter och har ett system för detta, DraftIT. På SLU:s hemsida för dataskydd & personuppgifter finns blankett och vägledning för anmälan om personuppgifter samt särskild information vad gäller personuppgifter i forskning.

[8] IA-system = Informationssystem om Arbetsmiljö.

Registersystemet hanteras av dataskyddsombudet och annan jurist på juristenheten. För att lägga in uppgifter i registret krävs särskild behörighet. För att underlätta för forskare beslutades[9] att anta särskilda rutiner för att dokumentera personuppgiftsbehandling inom forskningsprojekt där institution/motsvarande upprättar lokala förteckningar över de projekt som behandlar personuppgifter. Dataskyddsfunktionen har bistått institutionerna i att upprätta lokala register. På berörd institution ska det finnas en utsedd som ansvarig för att uppdatera de lokala registren. Det förekommer även registeruppställningar på centrala avdelningar i syfte att ha kontroll över hur personuppgifter hanteras och i vilka system.

*Registerförfrågan:*

SLU ska enligt GDPR se till att det finns information tillgänglig om hur registrerade personer ska gå till väga för att få registerutdrag eller begäran om radering av uppgifter. Sådan information är tillgängligt på såväl medarbetarwebben som studentwebben där det även finns kontaktuppgifter till dataskyddsombudet. Informationen finns på svenska, engelska samt för synskadade. Frågor från registrerade om personuppgifter har inkommit både till dataskyddsombudet och till andra verksamheter inom SLU. Frågorna har mest gällt registerutdrag men det har förekommit frågor (och begäran) om borttagning. Vid intervjuer framgår att inkomna frågor hänvisats vidare till dataskyddsombudet, som förmedlar frågan vidare till de verksamheter som kan ha uppgifter i sina system. Dataskyddsombudet sammanställer sedan uppgifterna och ger svar till registrerad. Det saknas dock processer och rutiner som beskriver hanteringen av registerförfrågan.

## 4.7 Överföring av uppgifter till tredje land

Genom GDPR har samtliga länder inom EU/EES ett likvärdigt skydd för personuppgifter och personlig integritet. Av den anledningen kan personuppgifter överföras fritt inom detta område. Däremot finns det inga generella regler utanför EU/EES som ger motsvarande garantier. Därför innehåller GDPR reglering för när personuppgifter får överföras till länder utanför EU/EES. Tidigare var det tillåtet att överföra personuppgifter till USA genom det s.k. Privacy Shield-avtalet mellan EU och USA. I juli 2020 avkunnade EU-domstolen en dom rörande överföring av personuppgifter till tredje land, den s.k. Schrems II-domen[10]. Domen innebär att Privacy Shield-avtalet förklarades vara i strid med EU-lagstiftning och upphävdes.

Schrems II-domen har medfört problem med överföring av personuppgifter till tredje land, inte bara för SLU och övriga lärosäten, utan generellt inom EU. När domen kom informerades SLU:s ledning om detta. Under hösten 2020 lade dataskyddsombudet ut rekommendationer om överföring till tredje land på

[9] Universitetsdirektörsbeslut. Rutiner för att dokumentera personuppgiftsbehandling inom forskningsprojekt i enlighet med dataskyddsförordningen, SLU.ua 2018.1.1.1-1921.
[10] Schrems II-domen – En EU-dom kring ändrade förutsättningar för tredjelandsöverföringar som handlar om förutsättningarna för laglig överföring av personuppgifter till USA och andra länder utanför EU.

Medarbetarwebben där det framgår vilka länder som enligt EU-kommissionen har lämplig skyddsnivå. Det finns även information om hur man inom SLU ska agera vid överföring av personuppgifter.

## 5. Analys och bedömning

Det finns ett antal styrande dokument på SLU:s hemsidor som anger hur personuppgifter ska hanteras inom SLU. Däremot saknas beskrivning av organisation och ansvarsfördelning för det centrala dataskyddsarbetet. SLU:s ansvar i egenskap av personuppgiftsansvarig särskiljs inte från dataskyddsombudets ansvar att övervaka efterlevnaden. Internrevisionen bedömer att det föreligger risk att dataskyddsombudets uppgifter blandas ihop med SLU:s ansvar. Dataskyddsfunktionens resurser omfattar både personuppgiftsansvarigs och dataskyddsombudets ansvarsområden. Detta försvårar möjligheten att särskilja dataskyddsombudets resursbehov i form av kompetens, stödresurser och tid.

Det har under granskningen påpekats att samma person inte kan göra både kontroller och informationsinsatser i egenskap av dataskyddsombud, då detta skulle påverka rollens oberoende enligt GDPR. Internrevisionen ser dock inget hinder enligt GDPR mot att ett datasskyddsombud utför samtliga moment inom övervakningsuppdraget, d.v.s. även informationsinsatser. Däremot kan flera personer utföra dataskyddsombudets uppgifter men det ska framgå vem som gör vad.

Dataskyddsombudet ska övervaka att SLU följer GDPR. Om det inte görs finns risk för att felaktig behandling av personuppgifter inte upptäcks och åtgärdas. Det har under granskningen framgått att dataskyddsfunktionen genomfört ett flertal informationsinsatser. Detta är viktigt för att öka medvetenheten om vad skydd av personuppgifter innebär. De övervakningsinsatser som genomförts utöver informationsinsatser har varit begränsade. De enkäter som gjorts har haft mycket låg svarsfrekvens och har endast i begränsad omfattning dokumenterats. Såvitt internrevisionen erfar har det därutöver inte gjorts andra uppföljande insatser, som intervjuer, stickprov etc. Internrevisionen bedömer att utan tydlig metod för övervakningsarbetet samt systematiska uppföljningsrutiner och god dokumentation är det svårt att bedöma hur väl SLU efterlever GDPR.

Att dataskyddsombudet ska rapportera till styrelsen framgår av GDPR. Rapportering gjordes av dataskyddsombudet 2019. Den rapport som lämnades 2020 var författad av en annan jurist. Rapporteringen 2021 genomfördes av dataskyddsombudet och bemöttes även av universitetsdirektören. Att rapporten bemöts av skriftliga kommentarer ser internrevisionen som en positiv utveckling. Det finns dock ingen formell rutin för hur brister som dataskyddsombudet påtalar ska hanteras. Detta riskerar leda till att noterade brister kvarstår.

Konsekvensbedömningar avseende dataskydd har enligt uppgift endast genomförts i begränsad omfattning. Information om konsekvensbedömningar och vägledning

brister. Informationen är svår att hitta i dataskyddshandböckerna vilket kan vara en anledning till att dataskyddombudet rådfrågats vid ett fåtal tillfällen. Dessa brister kan enligt internrevisionen leda till att personuppgifter hanteras felaktigt i exempelvis forskningsprojekt med risk för att SLU:s anseende skadas och tilldöms sanktionsavgifter. Dessutom riskerar den enskilde forskaren att inte kunna använda sitt material.

Rutinen för hanteringen av registerförfrågan innebär att den lämnas till dataskyddsombudet som är kontaktperson till den registrerade och lämnar förfrågning till de områden där det kan finnas registrerade uppgifter. Det saknas dock formell rutin för hantering av registerförfrågning. Detta innebär ett stort personberoende och kan leda till att felaktig information lämnas ut eller att personuppgifter hanteras felaktigt, exempelvis tas bort i strid med annan lagstiftning.

# 6. Rekommendationer

**Internrevisionen rekommenderar universitetsledningen att säkerställa**

**A**. att regelverket om dataskyddsförvaltning uppdateras så att gränsdragningen blir tydlig mellan verksamhetens ansvar att säkerställa att SLU som personuppgiftsansvarig följer GDPR och dataskyddsombudets ansvar att övervaka efterlevnaden. Det bör även framgå vilken roll dataskyddsombudet har vid exempelvis incidentrapportering och registerhantering.

**B.** att det finns tillräckliga resurser i form av kompetens, stödresurser och tid för dataskyddsombudet i enlighet med GDPR.

**C.** att dataskyddsombudets metod för övervakningsarbete, uppföljning och dokumentation förbättras för att öka kvaliteten i övervakning av SLU:s följsamhet mot GDPR.

**D.** att rutiner formaliseras för hur de brister som dataskyddsombudet rapporterar till styrelsen ska hanteras.

**E.** att verksamheten informeras om att konsekvensbedömningar avseende dataskydd ska genomföras. Dessutom bör informationen göras sökbar.

**F.** att rutiner för hantering av registerförfrågningar formaliseras.

Inga Astorsdotter
Internrevisionschef

Lisbeth Sundkvist Johansson
Internrevisor

# Rektors åtgärdsplan till internrevisionens rapport Hantering av dataskyddsförordningen.

| **Nr** | **Noterade brister**<br>(internrevisionen fyller i) | **Rekommendation**<br>(internrevisionen fyller i) | **Åtgärd**<br>(ledning/verksamhet fyller i) |
|---|---|---|---|
| A | Det saknas beskrivning av organisation och ansvarsfördelning för det centrala dataskyddsarbetet. SLU:s ansvar i egenskap av personuppgiftsansvarig särskiljs inte från dataskyddsombudets ansvar att övervaka efterlevnaden. Internrevisionen bedömer att det föreligger risk att dataskyddsombudets uppgifter blandas ihop med SLU:s ansvar. | Internrevisionen rekommenderar att universitetsledningen säkerställer att regelverket om dataskyddsförvaltning uppdateras så att gränsdragningen blir tydlig mellan verksamhetens ansvar att säkerställa att SLU som personuppgiftsansvarig följer GDPR och dataskyddsombudets ansvar att övervaka efterlevnaden. Det bör även framgå vilken roll dataskyddsombudet har vid exempelvis incidentrapportering och registerhantering. | **Ansvarig avdelning/enhet:** Ledningskansliet i samarbete med avdelningen för service, säkerhet och miljö<br><br>☒ Åtgärdas enligt rekommendation<br>☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan<br>☐ Åtgärdas inte, ange varför under kommentar nedan<br><br>**Kommentar:**<br><br>**Åtgärdas senast:** December 2021<br><br>**Dokumentation** (om det ej framgår ovan)**:** |
| B | Dataskyddsfunktionens resurser omfattar både personuppgiftsansvariges och dataskyddsombudets ansvarsområden. Detta försvårar möjligheten att särskilja | Internrevisionen rekommenderar att universitetsledningen säkerställer att det finns tillräckliga resurser i form av kompetens, stödresurser och tid för dataskyddsombudet i enlighet med GDPR. | **Ansvarig avdelning/enhet:** Ledningskansliet i samarbete med avdelningen för service, säkerhet och miljö |

| **Nr** | **Noterade brister**<br>(internrevisionen fyller i) | **Rekommendation**<br>(internrevisionen fyller i) | **Åtgärd**<br>(ledning/verksamhet fyller i) |
|---|---|---|---|
| | dataskyddsombudets resursbehov i form av kompetens, stödresurser och tid. | | ☒ Åtgärdas enligt rekommendation<br>☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan<br>☐ Åtgärdas inte, ange varför under kommentar nedan<br><br>**Kommentar:** När åtgärd A är åtgärdad kommer det finnas en tydligare bild av vilka resurser och ytterligare åtgärder som krävs.<br><br>**Åtgärdas senast:** April 2022<br><br>**Dokumentation** (om det ej framgår ovan)**:** |
| C | De övervakningsinsatser som genomförts utöver informationsinsatser har varit begränsade. De enkäter som gjorts har haft mycket låg svarsfrekvens och har endast i begränsad omfattning dokumenterats. Såvitt internrevisionen erfar har det därutöver inte gjorts andra uppföljande insatser, som intervjuer, stickprov etc. Internrevisionen bedömer att utan metod för övervakningsarbetet samt systematiska uppföljningsrutiner och god dokumentation är det svårt att bedöma hur väl SLU efterlever GDPR. | Internrevisionen rekommenderar att universitetsledningen säkerställer att dataskyddsombudets metod för övervakningsarbete, uppföljning och dokumentation förbättras för att öka kvaliteten i övervakning av SLU:s följsamhet mot GDPR. | **Ansvarig avdelning/enhet:** Ledningskansliet<br><br>☐ Åtgärdas enligt rekommendation<br>☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan<br>☐ Åtgärdas inte, ange varför under kommentar nedan<br><br>**Kommentar:** Med en tydlig organisation kan metoder och rutiner skapas av DSO och ”datahanteringsgruppen”.<br><br>**Åtgärdas senast:** Oktober 2022<br><br>**Dokumentation** (om det ej framgår ovan)**:** |

| **Nr** | **Noterade brister**<br>(internrevisionen fyller i) | **Rekommendation**<br>(internrevisionen fyller i) | **Åtgärd**<br>(ledning/verksamhet fyller i) |
|---|---|---|---|
| D | Det finns ingen formell rutin för hur brister som dataskyddsombudet påtalar ska hanteras. Detta riskerar leda till att noterade brister kvarstår. | Internrevisionen rekommenderar att universitetsledningen säkerställer att rutiner formaliseras för hur de brister som dataskyddsombudet rapporterar till styrelsen ska hanteras. | **Ansvarig avdelning/enhet:** Ledningskansliet<br><br>☐ Åtgärdas enligt rekommendation<br>☒ Åtgärdas på annat sätt, ange vilket under kommentar nedan<br>☐ Åtgärdas inte, ange varför under kommentar nedan<br><br>**Kommentar** Med en tydlig organisation kan metoder och rutiner skapas av DSO och ”datahanteringsgruppen”.<br><br>**Åtgärdas senast:** Oktober 2022<br><br>**Dokumentation** (om det ej framgår ovan)**:** |
| E. | Konsekvensbedömningar avseende dataskydd har enligt uppgift endast genomförts i begränsad omfattning. Information om konsekvensbedömningar och vägledning brister. Detta kan leda till att personuppgifter hanteras felaktigt i exempelvis forskningsprojekt med risk för att SLU:s anseende skadas och tilldöms sanktionsavgifter. Dessutom riskerar den enskilde forskaren att inte kunna använda sitt material. | Internrevisionen rekommenderar att universitetsledningen säkerställer att verksamheten informeras om att konsekvensbedömningar avseende dataskydd ska genomföras. Dessutom bör informationen göras sökbar. | **Ansvarig avdelning/enhet:** Ledningskansliet<br><br>☒ Åtgärdas enligt rekommendation<br>☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan<br>☐ Åtgärdas inte, ange varför under kommentar nedan<br><br>**Kommentar:** Med rätt resurser och en tydlig organisation kan utbildningsinsatser och stöd ges i större omfattning.<br><br>**Åtgärdas senast:** Oktober 2022<br><br>**Dokumentation** (om det ej framgår ovan)**:** |

| **Nr** | **Noterade brister**<br>(internrevisionen fyller i) | **Rekommendation**<br>(internrevisionen fyller i) | **Åtgärd**<br>(ledning/verksamhet fyller i) |
|---|---|---|---|
| F. | Det saknas formell rutin för hantering av registerförfrågningar. Detta kan leda till att felaktig information lämnas ut eller att personuppgifter hanteras felaktigt, exempelvis tas bort i strid med annan lagstiftning. | Internrevisionen rekommenderar att universitetsledningen säkerställer att rutiner för hantering av registerförfrågningar formaliseras. | **Ansvarig avdelning/enhet:** Ledningskansliet<br><br>☒ Åtgärdas enligt rekommendation<br>☐ Åtgärdas på annat sätt, ange vilket under kommentar nedan<br>☐ Åtgärdas inte, ange varför under kommentar nedan<br><br>**Kommentar:**<br><br>**Åtgärdas senast:** Februari 2022<br><br>**Dokumentation** (om det ej framgår ovan)**:** |