UPPSALA UNIVERSITET

UFV 2022/806

Dataskyddsarbete –

Dataskyddsförordningen (GDPR)

Internrevisionsrapport

Fastställd av Konsistoriet 2022-12-14

Innehållsförteckning

Sammanfattning

Internrevisionen har granskat om universitetets dataskyddsarbete bedrivs med god intern styrning och kontroll och att rutiner för personuppgiftsbehandling är utformade i enlighet med de krav som ställs i dataskyddsförordningen. Granskningen har särskilt inriktats på följande områden: ansvar, roller och styrande dokument, kunskap, information och stöd, uppföljning och övervakning samt rapportering.

En bristfällig hantering av personuppgifter riskerar att enskildas personuppgifter inte skyddas, att enskildas mänskliga rättigheter och friheter hotas samt att förtroendet för universitetet skadas. Vid överträdelser i förhållande till dataskyddsförordningen riskeras dessutom avsevärda skadestånd och sanktionsavgifter.

Granskningen visar att det, trots det omfattande arbete som hittills genomförts för att implementera dataskyddsförordningen inom universitetets organisation, krävs ytterligare åtgärder i förhållande till de krav som ställs i dataskyddsförordningen samt för att uppnå god intern styrning och kontroll.

Brister som internrevisionen har iakttagit i förhållande till dataskyddsförordningen är att:

- roll- och ansvarsfördelningen mellan dataskyddsombudet och universitetet som personuppgiftsansvarig inte är tillräckligt tydliggjord och separerad,
- dataskyddsombudet kan följaktligen inte upprätthålla en oberoende tillsynsroll,
- dataskyddsombudet inte arbetar med övervakning av att dataskyddsförordningen följs trots att det är en av huvuduppgifterna enligt dataskyddsförordningen och
- att det saknas en etablerad rutin för regelbunden rapportering från dataskyddsombudet till högsta förvaltningsnivå.

Därtill visar granskningen att det saknas universitetsövergripande styrdokument som beskriver hur universitetets dataskyddsarbete ska vara organiserat, roll- och ansvarsfördelning, arbetsuppgifter samt rutiner för uppföljning, övervakning och rapportering. Det har även noterats ett behov av förstärkta och målgruppsanpassade informations- och utbildningsinsatser.

Internrevisionens sammanfattande bedömning är att ett stort förbättringsbehov föreligger och internrevisionen lämnar därför ett antal rekommendationer till rektor, i syfte att universitetets arbete med behandling och skydd av personuppgifter ska kunna utformas i enlighet med krav i dataskyddsförordningen och med god intern styrning och kontroll.

1 Bakgrund

EU:s dataskyddsförordning General Data Protection Regulation, GDPR, som trädde i kraft den 25 maj 2018 innebär strikta krav på behandling av personuppgifter. [1] Det ställs i förordningen höga krav på rutiner för säker hantering och skydd av personuppgifter. En bristfällig hantering av personuppgifter riskerar att enskildas personuppgifter inte skyddas, att enskildas mänskliga rättigheter och friheter hotas samt att förtroendet för universitetet skadas. I de fall universitetet brister i regelefterlevnad riskeras dessutom avsevärda skadestånd och sanktionsavgifter. [2] I enlighet med revisionsplanen genomför internrevisionen en granskning av universitetets processer och rutiner kopplat till personuppgiftsbehandling i syfte att bedöma regelefterlevnaden av dataskyddsförordningen samt den interna styrningen och kontrollen.

2 Syfte och omfattning

Syftet med granskningen är att undersöka och bedöma om universitetets dataskyddsarbete och rutiner för behandling av personuppgifter är utformade i enlighet med krav som ställs i dataskyddsförordningen samt med god intern styrning och kontroll. Granskningen har inriktats på följande områden:

- ansvarsfördelning, roller och styrande dokument,
- kunskap, information och stöd,
- uppföljning och övervakning samt
- rapportering.

Granskningen har genomförts genom dokumentstudier och intervjuer. Intervjuer har hållits med universitetets dataskyddsombud och den universitetsjurist vid Juridiska avdelningen som arbetar tillsammans med dataskyddsombudet. Intervjuer har även hållits med ordföranden för konsistoriet, universitetsdirektören, akademiombudsmannen, chefen för Enheten för informationssäkerhet vid Säkerhetsavdelningen samt upphandlingschefen vid Avdelningen för ekonomi och upphandling. I syfte att fånga upp erfarenheter av det dataskyddsarbete som utförs inom organisationen, har även prefekter och medarbetare med arbetsuppgifter kopplat till personuppgiftsbehandling vid Institutionen för Kirurgiska vetenskaper, Institutionen för Psykologi och Institutionen för Läkemedelskemi intervjuats och bidragit med information.

Dataskyddsarbetet som sker enligt dataskyddsförordningen och de informationssäkerhets-åtgärder som utformas för att skydda personuppgifter, utgör en del av universitetets informationssäkerhetsarbete. [3] Internrevisionen har tidigare – under 2021 – genomfört en granskning av universitetets informationssäkerhetsarbete utifrån de krav som MSB via föreskrifter ställer på myndigheters informationssäkerhetsarbete. Då avgränsades dock

[1] Fr o m den 25 maj 2018 tillämpas EU:s dataskyddsförordning 2016/679 (engelsk akronym GDPR, härefter främst benämnd dataskyddsförordningen) om skydd för fysiska personer m a p behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, som lag i alla EU:s medlemsländer. Sverige har även beslutat om kompletterande nationell lagstiftning, bl.a. genom dataskyddslagen (2018:218) som också trädde i kraft 25 maj 2018. Samma dag upphävdes personuppgiftslagen PuL (1998:204).

[2] Enligt information på Integritetsskyddsmyndighetens webbplats kan t.ex. sanktionsavgifter vad avser myndigheters överträdelser uppgå till maximalt 10 miljoner kronor.

[3] Med dataskyddsarbete avses i det följande de rutiner och processer som universitetet etablerat kopplat till behandling av personuppgifter som sker på basis av krav i dataskyddsförordningen.

granskningen från informationstyper som lyder under separata lagstiftningar såsom personuppgifter – GDPR/dataskyddsförordningen.

2.1 Revisionsfrågor

För att uppnå syftet kommer följande revisionsfrågor att besvaras:

- Är ansvarsfördelning och roller för dataskyddsarbetet tydliggjorda (personuppgiftsansvarig, personuppgiftsbiträde, dataskyddsombud)?
- Finns styrande dokument som tydliggör hur arbetet med personuppgiftsbehandling och dataskydd är organiserat och ska bedrivas inom universitetet, t.ex. ansvarsfördelning, roller, arbetsuppgifter, hur det ska styras, följas upp, övervakas och rapporteras?
- Vilken information, utbildning och stöd tillhandahåller universitetet medarbetare och studenter som hanterar personuppgifter?
- Finns rutiner för uppföljning och övervakning av att dataskyddsförordningen efterlevs och av att universitetets rutiner och strategi för dataskydd av personuppgifter är implementerade och tillämpas?
- Finns rapporteringsrutiner så att högsta förvaltningsnivå får återrapportering?

2.2 Risker

Brister i universitetets behandling och dataskydd av personuppgifter riskerar att leda till:

- att enskilda individers personuppgifter inte skyddas när de behandlas av universitetet,
- att förtroendet för universitetet och dess verksamhet skadas,
- sanktionsavgifter och skadestånd vid felaktig behandling av personuppgifter.

2.3 Bedömningskriterier

Med bedömningskriterier avses de regelverk och normer som bildar underlag för internrevisionens bedömningar och rekommendationer. Granskningen tar sin utgångspunkt i och bedömningar görs utifrån myndighetsförordningens krav om att verksamheten ska bedrivas på ett sätt så att bl.a. effektivitet, regelefterlevnad och god hushållning med medel uppnås samt högskoleförordningens krav på att det vid universitetet ska finnas en intern styrning och kontroll som fungerar på ett betryggande sätt. [4]

Bedömningar görs därutöver utifrån dataskyddsförordningen samt interna styrdokument. [5]

[4] 3 § Myndighetsförordningen (2007:515) och 2 kap. 2 § högskoleförordningen (SFS 1993:100).

[5] EU:s dataskyddsförordning 2016/679 (GDPR) och internt styrdokument såsom: Rutiner för informationssäkerhet vid Uppsala universitet (UFV 2017/93) samt information om dataskyddsförordning m.m. på universitetets medarbetarportal (mp).

3 Iakttagelser och resultat från granskningen

I kapitel 3 redogörs för iakttagelser och bedömningar som gjorts under granskningen. [6] Rapporteringen är i huvudsak avvikelsebaserad vilket innebär att sådana iakttagelser som vi bedömer som brister eller risker beskrivs.

3.1 Ansvarsfördelning och roller samt styrande dokument

Granskningen visar att roll- och ansvarsfördelning mellan dataskyddsombudets oberoende tillsynsroll och universitetets operativa roll som personuppgiftsansvarig inte är tillräckligt tydliggjord och separerad i praktiken. Det saknas universitetsövergripande styrdokument som beskriver hur universitetets dataskyddsarbete är organiserat, roll- och ansvarsfördelning samt rutiner för uppföljning, övervakning och rapportering m.m.

Dataskyddsförordningen ställer krav på hur organisationer och myndigheters dataskyddsarbete ska utformas och styras, t.ex. att ansvar för dataskyddsarbetet och vissa roller, såsom personuppgiftsansvarig, personuppgiftsbiträde och dataskyddsombud, ska vara tydliggjorda. [7]

Uppsala universitet ansvarar för personuppgiftsbehandling som utförs inom universitetets verksamhet. Universitetet är som myndighet således *personuppgiftsansvarig* vid behandling av ”egna” personuppgifter och bestämmer för vilka ändamål de ska behandlas och hur behandlingen ska gå till. Som personuppgiftsansvarig ansvarar universitetet för att dataskyddsförordningen efterlevs och ska genomföra lämpliga tekniska och organisatoriska skyddsåtgärder, för att säkerställa och kunna visa att personuppgiftsbehandling inom verksamheten utförs i enlighet med förordningen. [8]

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning.[9] Som personuppgiftsansvarig ställs krav på att universitetet har avtal (personuppgiftsbiträdesavtal) med varje organisation (personuppgiftsbiträde) som behandlar personuppgifter som universitetet ansvarar för. [10]

Vidare ska universitetet som personuppgiftsansvarig myndighet, i enlighet med krav i dataskyddsförordningen, utnämna ett *dataskyddsombud*. [11] Dataskyddsombud är en oberoende och självständig tillsynsroll med primär uppgift att övervaka att dataskyddsförordningen och myndighetens strategi för skydd av personuppgifter efterlevs i organisationen. Till

[6] Iakttagelserna bygger huvudsakligen på uppgifter som inhämtats vid intervjuer och baseras därmed på de intervjuades beskrivningar av det egna arbetet och/eller verksamhetens rutiner. Intervjuerna har skett under vår/sommar 2022.

[7] Dataskyddsförordningen artikel 24-29 och 37-39.

[8] Dataskyddsförordningen artikel 5 p. 1 och p. 2, artikel 12, artikel 24 m.fl.

[9] Dataskyddsförordningen artikel 28. Definition av personuppgiftsbiträde framgår av artikel 4 p.8: en fysisk eller juridisk person, offentlig myndighet, institution/organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

[10] På medarbetarportalen – mp.uu.se/web/info/forska/forskningsavtal/gdpr-och-underbitraden – finns universitetets rutin för upprättande av personuppgiftsbiträdesavtal beskriven och det finns även en avtalsmall som stöd vid avtalstecknande. Det förekommer även det omvända – att universitetet är biträde och i de fallen används samma avtalsmall. I fall av eventuella avvikelser från mallen ska avtalet granskas av Juridiska avdelningen innan det tecknas (och hänskjutas till universitetsdirektören om avvikelserna är av principiell betydelse). Juridiska avdelningen bistår även med rådgivning vid upprättande av personuppgiftsbiträdesavtal. Personuppgiftsbiträdesavtalen registreras i W3D3. Personuppgiftsbiträdesrollen har inte varit fokus för internrevisionens granskning och därför har inte tillämpningen av dessa rutiner granskats vidare.

[11] Dataskyddsförordningen artikel 37.

dataskyddsombudets uppgifter hör även att informera och ge råd till myndigheten och de anställda som behandlar personuppgifter, om deras skyldigheter enligt förordningen och annan dataskyddslagstiftning. Den personuppgiftsansvarige ska säkerställa dataskyddsombudets ställning, bl.a. genom att tillhandahålla de resurser som krävs för att fullgöra uppgifterna, se till att dataskyddsombudet på ett korrekt sätt och i god tid bereds möjlighet att delta i frågor som rör skydd av personuppgifter samt se till att andra uppgifter/uppdrag som dataskyddsombudet utför inte leder till en intressekonflikt. [12]

Uppsala universitet har, sedan införandet av dataskyddsförordningen 2018, ett dataskyddsombud anställt vid myndigheten. [13] Organisatoriskt är dataskyddsombudet placerat vid Juridiska avdelningen inom universitetsförvaltningen. Därutöver finns en ytterligare personell resurs till hjälp i dataskyddsombudets arbete, genom att en av universitetsjuristerna vid Juridiska avdelningen arbetar deltid med GDPR tillsammans med dataskyddsombudet. Dataskyddsombudet är, vid sidan av dataskyddsombudsrollen, även enhetschef vid Juridiska avdelningens Enhet för informationsförsörjning, registratur och arkiv. [14]

Internrevisionen noterar att det inte är specificerat hur stor del av deras respektive arbetstid som ska ägnas åt GDPR/dataskyddsverksamhet. Inte heller arbetsuppgifter och ansvarsfördelning är klargjord dem emellan. Dataskyddsombudets roll finns angiven i universitetets informationssäkerhetspolicy, dock noterar internrevisionen att det i policyn inte finns vidare kopplingar till krav som ställs enligt dataskyddsförordningen. [15] I övrigt saknas styrande dokument (arbetsordning, instruktion, riktlinjer eller liknande) som beskriver hur det universitetsgemensamma dataskyddsarbetet är organiserat, roll- och ansvarsfördelning, vilka arbetsuppgifter som ska utföras av dataskyddsombudet respektive personuppgiftsansvarig, rutiner för uppföljning, övervakning och rapportering o.s.v.

Dataskyddsombudet och universitetsjuristen beskriver vid intervjuer att de, sedan förordningens införande 2018, fokuserat arbetet på att utveckla rutiner och arbetssätt samt på information och rådgivning till de som behandlar personuppgifter vid institutioner och andra delar av universitetets organisation. Det framgår av granskningen att det inte finns rutiner för uppföljning av den behandling av personuppgifter som sker ute i organisationen, vare sig hos dataskyddsombudet eller på universitetet som personuppgiftsansvarig. Dataskyddsombudet uppger att han inte överhuvudtaget arbetar med övervakning, tillsyn eller kontroll av att

[12] Dataskyddsförordningen artikel 37-39 samt information om dataskyddsombud på tillsynsmyndigheten/IMY:s webbplats. Vad avser övervakning kan detta exempelvis ske genom att samla in information om hur organisationen behandlar personuppgifter samt genom tillsyn och att utföra utvärderingar och kontroller.

[13] I enlighet med kraven i dataskyddsförordningen artikel 37 p. 7 har universitetet meddelat tillsynsmyndigheten, Datainspektionen (numera Integritetsskyddsmyndigheten IMY), vem som är utnämnd till dataskyddsombud och offentliggjort ombudets kontaktuppgifter både på universitetets externa och interna webbplats. Se dnr UU-DsO 2018/2.

[14] Arbetsrollen som enhetschef för Enheten för informationsförsörjning, registratur och arkiv innebär arbetsledning av enhetens sex medarbetare.

[15] Rutiner för informationssäkerhet, UFV 2017/93, reviderad 2021-03-23. Informationssäkerhetspolicyn beskriver säkerhetskrav som ställs på all behandling av information och är främst skriven utifrån krav som MSB genom föreskrifter ställer på statliga myndigheter. Dataskyddsombudsrollen finns omnämnd men i övrigt är inte policyn skriven med hänsyn till krav som ställs enligt annan lagstiftning, t.ex. GDPR/Dataskyddsförordningen. Som exempel beskrivs endast att incidenter ska anmälas till MSB men inte att personuppgiftsincidenter ska anmälas till IMY samt att det i avsnittet om uppföljning och rapportering inte står något om att dataskyddsombudet ska rapportera till högsta förvaltningsnivå/konsistoriet.

dataskyddsförordningen och universitetets strategi för dataskydd efterlevs, trots att det enligt förordningen är en av dataskyddsombudets huvuduppgifter.[16]

Dataskyddsombudet beskriver vidare att det dagliga arbetet i hög utsträckning är av operativ karaktär och att han i praktiken, trots den oberoende tillsynsrollen, bereder och hanterar operativa universitetsgemensamma personuppgifts- och dataskyddsärenden.[17]

Enligt den handlingsplan som upprättades av Juridiska avdelningen i samband med implementeringen av dataskyddsförordningen 2018, var en av aktiviteterna att tillsätta en framtida förvaltningsorganisation för att säkerställa efterlevnad av dataskyddsförordningen och att tydliggöra roller och ansvar.[18] Internrevisionen konstaterar dock att arbete kvarstår med att tydliggöra roller och ansvarsfördelning. Universitetet som personuppgiftsansvarig har inte heller någon central förvaltande dataskyddsorganisation etablerad eller resurs utsedd att arbeta med den personuppgiftsansvariges operativa universitetsgemensamma uppgifter.

Granskningen visar att universitetets dataskyddsombud i praktiken har dubbla roller som är svåra att förena. Dataskyddsombudet utför arbete inom sin tillsynsroll, men är samtidigt i hög grad involverad i det praktiska operativa arbetet. Detta riskerar att leda till att dataskyddsombudet inte kan upprätthålla ett oberoende förhållningssätt i sin granskande tillsynsroll, i fall då han exempelvis kan komma att behöva granska rutiner, arbetssätt och verktyg som han själv byggt upp eller granska principiella ställningstaganden och ärenden som han själv berett och hanterat. Internrevisionen bedömer att detta inte är en tillfredställande segregering av arbetsuppgifter och ser ett behov av att ansvarsfördelning och roller tydliggörs så att, de nu sammanblandade rollerna, i högre grad separeras.[19]

Dataskyddsarbetet och hur personuppgifter ska hanteras inom organisationen styrs genom dataskyddsförordningen. Internrevisionen ser dock ett behov av att utveckla styrningen av det universitetsgemensamma dataskyddsarbetet, både i syfte att förbättra den interna styrningen och kontrollen samt för att uppnå ökad regelefterlevnad i förhållande till dataskyddsförordningen. Styrningen bör utvecklas och dokumenteras genom framtagande av ett universitetsövergripande styrdokument som:

- beskriver hur arbetet med personuppgiftsbehandling och dataskydd är organiserat,
- tydliggör roller, ansvarsfördelning och arbetsuppgifter,
- klargör en central förvaltande dataskyddsorganisation,
- klargör rutiner för hur dataskyddsombudets övervakande uppgifter ska utföras samt
- klargör rutiner för hur systematisk och strukturerad uppföljning, övervakning och rapportering ska ske.

[16] Utöver den inblick i verksamhetens personuppgiftsarbete som dataskyddsombudet får genom rådgivningsverksamheten.

[17] Exempel på operativa uppgifter som dataskyddsombudet utför (trots att hans roll är en oberoende, granskande tillsynsroll) men som borde utföras inom ramen för den operativa personuppgiftsansvarigrollen är bl.a. praktisk förvaltning av personuppgiftsregistret, utveckling av rutiner, arbetssätt, metoder, mallar m.m. samt beredning och hantering av operativa universitetsgemensamma personuppgifts- och dataskyddsärenden och frågor.

[18] Handlingsplan för dataskyddsförordningen - anpassning Uppsala universitet, Dnr 2017/1034.

[19] Myndigheten ska enligt dataskyddsförordningen ha ett utnämnt dataskyddsombud. På Integritetsskyddsmyndighetens (IMY) webbplats framgår dock olika förslag till lösningar för att hålla rollerna separerade. En lösning är exempelvis att anlita ett externt dataskyddsombud (extern tjänsteleverantör) för att utföra tillsyns- och övervakningsuppgifterna.

Ett förbättringsbehov som framkommit under granskningen, och som är kopplat till dataskyddsombudets ställning, är också att det bör säkerställas att dataskyddsombudet systematiskt och i god tid involveras i sådana processer där principiella dataskyddsfrågor rörande skydd av personuppgifter ofta aktualiseras och som kan kräva bedömning och råd utifrån regelefterlevnadsaspekt. Exempelvis kan sådana dataskyddsfrågor aktualiseras inför beslut om inköp/upphandling av IT-lösningar och inför användning av molnbaserad IT-tjänst. [20]

Internrevisionen har även noterat brister vad avser systematik och struktur i styrningen och genomförandet av det universitetsgemensamma dataskyddsarbetet, informations-, stödjande- och utvecklingsinsatser m.m. vilket riskerar medföra negativ påverkan utifrån ett effektivitetsperspektiv. Arbetet förefaller inte planeras och styras strukturerat och systematiskt. Exempelvis har vi inte kunnat finna dokumentation som visar att det utförs efter planerade strategier, årlig plan eller med prioritering av aktiviteter och utvecklingsinsatser på kort och lång sikt. Internrevisionen bedömer att det finns ett förbättringsbehov även här.

3.2 Kunskap, information och stöd

Granskningen visar att det finns behov av förstärkta informations- och utbildningsinsatser för att öka kunskapen om personuppgiftsbehandling och dataskydd hos universitetets medarbetare och studenter. Informationsmaterial och vägledande dokument på medarbetarportalen bör i ännu högre grad förenklas och målgruppsanpassas för att öka möjligheten att nå fram med budskapet och underlätta för dem som arbetar med personuppgiftsbehandling.

Kunskap om dataskyddsförordningen, väl fungerande interna rutiner samt information och stöd som behövs för arbetet, är förutsättningar för att personuppgifter ska kunna behandlas och skyddas på ett säkert sätt. I fall då kunskap och medvetenhet om dataskyddsförordningen/ GDPR är otillräcklig kan det leda till att enskildas personuppgifter inte skyddas i enlighet med kraven i dataskyddsförordningen.

Uppsala universitet är som myndighet personuppgiftsansvarig och ansvarar därmed för att dataskyddsförordningen efterlevs och att medarbetarna får information och har tillräckliga kunskaper om regler och rutiner. En av dataskyddsombudets uppgifter, enligt dataskyddsförordningen, är att ge information och råd till den personuppgiftsansvarige och de anställda om deras skyldigheter enligt förordningen. [21]

På universitetets medarbetarportal finns information samlad om dataskyddsförordningen och de interna arbetssätt som gäller för personuppgiftsbehandling och dataskyddsarbete inom universitetet. Där finns även en dataskyddspolicy med information riktad till de registrerade om hur och enligt vilka principer universitetet behandlar personuppgifter, samt vägledande dokument, blanketter, mallar och rutiner som dataskyddsombudet utvecklat till stöd för medarbetarna i deras arbete. Exempelvis finns en rutin för anmälan av personuppgiftsbehandling med en tillhörande elektronisk anmälningsblankett, som vid

[20] Under granskningen har det framkommit exempel där beslut om inköp eller val av IT-lösning enligt uppgift riskerar leda till regelöverträdelse gällande dataskyddsförordningen, bl.a. användande av Teams, inköp av molntjänst för universitetsbibliotekets in- och utlån och upphandling av transkriberingstjänster. Dessa hade kunnat undvikas om dataskyddsombudet systematiskt och i tid involverats och/eller att de råd som dataskyddsombudet lämnat följts.

[21] Dataskyddsförordningen artikel 39 p.1 a.

användning innebär att anmälan registreras i en särskild diarieserie i W3D3 som utgör universitetets personuppgiftsbehandlingsregister. Registret är ett krav i dataskyddsförordningen. Där finns också elektroniska blanketter för anmälan av personuppgiftsbiträde, anmälan av studenters personuppgiftsbehandling, inventeringsblankett för kartläggning och dokumentation av tredjelandsöverföringar av personuppgifter m.m. [22]

På medarbetarportalen finns även kontaktuppgift till dataskyddsombudets funktionsepostlåda, vilken är en av ingångarna för institutioner och andra verksamheter som är i behov av stöd och rådgivning. Där finns även länkar till nära angränsande områden som bl.a. informationssäkerhet och etikprövning. [23]

Vad gäller informations- och rådgivningsinsatser beskriver dataskyddsombudet och universitetsjuristen, som tidigare nämnts, att deras informations- och rådgivningsinsatser i hög grad genomförs efterfrågebaserat och reaktivt utifrån inkomna frågor och aktuella problem. Situationen beskrivs som att de: ”står i skyttegraven och skyfflar svar på inkommande frågor”.[24] Enligt uppgift utförs varken deras stödjande arbete eller det universitetsövergripande arbetet med personuppgiftsbehandling och dataskydd i övrigt, strukturerat och systematiskt, t.ex. via målinriktat arbete med verksamhetsplanering, aktiviteter och prioriteringar på kort och lång sikt eller uppföljning och utvärdering av genomförda insatser. Vid införandet av dataskyddsförordningen genomfördes dock informationsinsatser mer systematiskt, då dataskyddsombudet tillsammans med informationssäkerhetssamordnarna vid Säkerhets-avdelningen, gemensamt höll workshops vid institutioner, forskningsprojekt m.fl. för att öka medvetenheten om personuppgiftshantering och dataskyddsförordningen. Internrevisionen noterar att institutionerna som intervjuats uppger att de, i huvudsak varit mycket nöjda med stöd, råd och vägledning som de fått i kontakter med dataskyddsombudet, universitetsjuristen, Juridiska avdelningen och informationssäkerhetssamordnarna vid Säkerhetsavdelningen.

Internrevisionen noterar att det vid universitetet inte finns återkommande/reguljära informationstillfällen och inte heller någon internutbildning/-kurs specifikt inriktad på att ge medarbetarna grundläggande kunskaper om skyldigheter enligt dataskyddsförordningen och hur behandling av personuppgifter får göras inom universitetet.[25] Enligt den handlingsplan som upprättades av Juridiska avdelningen i samband med implementeringen av dataskyddsförordningen var en av aktiviteterna att fortsätta arbetet med att öka medvetenheten om förordningen i organisationen, bl.a. genom att ta fram ett långsiktigt och tydligt informations- och utbildningsprogram. [26] Internrevisionen noterar att detta inte genomförts.

[22] Medarbetarportalen - mp.uu.se/web/info/stod/dataskyddsforordningen. Dataskyddspolicy – Behandling av personuppgifter vid Uppsala universitet, senast ändrad 2018-05-09. Personuppgiftsregister benämns i det följande registerförteckning.

[23] Medarbetarportalen - mp.uu.se/web/info/stod/dataskyddsforordningen men även webbplatser i anslutning till andra områden, t.ex. Informationssäkerhet (då personuppgifter är en av de informationstyper som ska skyddas utifrån krav som ställs på myndigheters informationssäkerhet, och samarbete därför är etablerat med universitetets informationssäkerhetssamordnares stödjande verksamhet), Etikprövning (då etikgodkännande krävs vid behandling av vissa känsliga personuppgifter inom forskning), Forskningsdata & IT/Fillagring (då säkra tekniska lösningar för att lagra och dela personuppgifter behövs).

[24] Informations- och rådgivningsinsatser bl.a. via funktionsepostlådan, möten och i andra kontakter inom organisationen.

[25] I universitetets internutbildningsutbud finns dock kurser med inslag kopplat till personuppgiftshantering och dataskydd, t.ex. i kursen Informationssäkerhet – det händer inte mig och Handledning av doktorander.

[26] Handlingsplan för dataskyddsförordningen - anpassning Uppsala universitet, Dnr 2017/1034.

Vid institutionsintervjuer har flera av de som intervjuats lyft behovet av *kontinuerliga* informationsinsatser, påminnelser om gällande regler samt tillgång till centralt tillhandahållen målgruppsanpassad internutbildning för dataskyddsområdet. I universitetets decentraliserade organisation är det idag upp till varje institution, prefekt, forskningsgruppsledare o.s.v. att utforma sin egen information och introduktion till dataskyddsförordningen, t.ex. för nyanställda, inför start av forskningsstudie/-projekt, för studenter inför examensarbete, riktad till olika administrativa roller såsom HR-administratörer, studie-/kursadministratörer m.fl.

Vid ett par av institutionsintervjuerna noteras även att den befintliga webbinformationen om personuppgiftsbehandling och dataskydd på medarbetarportalen, i vissa delar upplevs tung, teknisk och detaljerad. Texten upplevs svår och tidskrävande att sätta sig in i, praktiskt tillämpa och göra bedömningar utifrån för enskilda medarbetare, som kanske dessutom är s.k. sällananvändare. Informationen skulle enligt de som intervjuats vinna på att göras mer användarvänlig, koncis, förenklad och processinriktad som ”gör så här” eller ”steg för steg”. Det har även framförts önskemål om att information och vägledning i ännu högre grad bör målgruppsanpassas och riktas till olika roller, gärna med vägledande FAQ avseende den praktiska tillämpningen. [27] Under granskningen har det framkommit att forskare och doktorander inom det medicinsk-farmaceutiska vetenskapsområdet, som har dubbla anställningar har särskilda utmaningar vad gäller behandling av personuppgifter. De kan tjänstgöra och samla in känsliga personuppgifter/medicinska data i rollen vid Akademiska sjukhuset på förmiddagen och sedan på eftermiddagen forska på de insamlade person-uppgifterna i sin roll som forskare vid universitetet. Det förekommer därvidlag att de arbetar i helt olika datamiljöer och det innebär att personuppgifter rör sig mellan två olika juridiska personer, vilket kräver medvetenhet om att sådan överföring måste prövas och regleras. Samma problem kan även uppstå för associerade medarbetare vid forskningssamarbeten. Vidare har internrevisionen vid institutionsintervjuer noterat att kännedomen är låg om att även studenters behandling av personuppgifter, t.ex. inom ramen för examensarbeten, ska anmälas till den särskilda registerförteckning som tagits fram av dataskyddsombudet för personuppgifts-behandling. Under internrevisionens tidigare granskning av den generella informations-säkerheten gjordes även iakttagelser som indikerar bristande kännedom om regler för personuppgiftsbehandling. Som exempel iakttogs uppfattningen att om en forskare har lämnat in en etikprövning och fått ett etikgodkännande så krävs ingen vidare personuppgiftsanmälan. En uppfattning som även dataskyddsombudet uppger att han möts av och som är felaktig.

Internrevisionen konstaterar att det på universitetets medarbetarportal finns ett omfattande informationsmaterial, automatiserade arbetsflöden, elektroniska anmälningsblanketter och andra stödjande och vägledande dokument. För att ytterligare förenkla och underlätta för institutioner och medarbetare som behandlar personuppgifter att följa dataskyddsförordningen, bedömer internrevisionen att det finns förbättringspotential. Informationsmaterial kan i ännu högre grad än nu göras användarvänligt och stödjande för prefekter och användare genom att materialet målgruppsanpassas och riktas till olika roller. Respondenter har vid intervjuer även efterlyst centrala vägledande ställningstaganden och principer från den personuppgiftsansvarige

[27] Exempelvis: Hur hanterar och bemöter jag, som studie-/kursadministratör, när jag får inkommande e-post med personuppgifter och känsliga uppgifter om hälsa från studenter? Hur gör jag som forskare när jag måste delta i en internationell konferens i tredjeland när anmälan kräver att jag lämnar namn, e-postadress och andra personuppgifter via molnbaserade it-lösningar? Hur hanterar jag, som har dubbla anställningar (UU och Akademiska sjukhuset), personuppgifter när rutinerna skiljer sig åt och systemen i de olika organisationerna inte är kompatibla?

för vad som är tillåtet/inte tillåtet och hur konkreta situationer kan lösas. [28] Internrevisionen ser även ett behov av förstärkta och kontinuerliga informations- och utbildningsinsatser för att öka kunskapen om personuppgiftsbehandling och dataskydd hos universitetets medarbetare och studenter. [29] Brister i form av att inte nå ut med kunskap och information riskerar leda till att personuppgifter lämnas ut, sprids eller på annat sätt hanteras felaktigt och i strid med dataskyddsförordningen. Utöver risken att förtroendet för universitetet kan skadas, kan brister i hantering och dataskydd av personuppgifter, i ett forskningsprojekt även innebära risker såsom att den enskilde forskarens forskningsmaterial inte får användas vidare i studien/projektet eller att det påverkar möjligheten till vidare forskningsfinansiering. Ett annat riskområde vid hantering av forskningsdata kopplat till personuppgiftsbehandling gäller publicering av resultat och öppna data. Det kan som exempel röra sig om att vetenskapliga publicister kräver öppen tillgång till forskningsdata inför en publicering och att det kan innebära att personuppgifter delas i strid med dataskyddsförordningen.

3.3 Uppföljning och övervakning

Granskningen visar att varken uppföljning, övervakning eller kontroll genomförs av universitetets arbete med personuppgiftsbehandling eller att dataskyddsförordningen efterlevs. Universitetet som personuppgiftsansvarig myndighet saknar former för uppföljning av att dataskyddsförordningen följs och att interna rutiner är implementerade och tillämpas inom organisationen. Dataskyddsombudet saknar rutiner för övervakning, tillsyn och kontroll av att dataskyddsförordningen och den personuppgiftsansvariges strategi för dataskydd efterlevs, trots att det enligt dataskyddsförordningen är en av dataskyddsombudets huvuduppgifter.

Rollen som dataskyddsombud innebär en självständig och oberoende tillsynsroll i förhållande till den personuppgiftsansvariges verksamhet.[30] En av dataskyddsombudets huvuduppgifter är att övervaka efterlevnaden av dataskyddsförordningen och den personuppgiftsansvariges strategi för dataskydd.[31] Uppföljning och övervakning är även väsentliga beståndsdelar av ett systematiskt dataskyddsarbete och den interna styrningen och kontrollen, då det bidrar till att ge en lägesbild av om arbetet med att skydda enskilda individers personuppgifter fungerar på avsett sätt och om dataskyddsförordningen och interna rutiner är implementerade och efterlevs.

[28] Brist på centrala vägledande ställningstaganden och principer kan, i universitetets decentraliserade organisation, medföra risk att prefekter, forskningsgruppsledare, forskare och andra enskilda medarbetare ska göra kvalificerade bedömningar av frågor själva trots att de ibland besitter mer begränsad kunskap än den ”specialistkunskap” som finns samlad vid universitetet centralt. Exempel kan vara ställningstagande och konkreta lösningar till väsentliga frågor med betydelse för regelefterlevnaden av dataskyddsförordningen/GDPR t.ex. hur studenters behandling av personuppgifter vid examensarbeten ska hanteras, vilka molnbaserade tjänster som får nyttjas/inte ska nyttjas, vilken transkriberingstjänst som ska nyttjas o.s.v.

[29] Vad avser studenter kan information om GDPR ges t.ex. inför påbörjande av examensarbete eller datainsamlingar.

[30] Av Integritetsskyddsmyndighetens webbplats framgår: ”Ombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.” och ”Dataskyddsombudet ska kunna arbeta självständigt och oberoende, utan att bli påverkad av andra inom organisationen” samt att ”Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvariga eller hos personuppgiftsbiträdet.”.

[31] Enligt dataskyddsförordningen artikel 39 ska dataskyddsombudet ha minst följande uppgifter: bl.a. övervaka efterlevnad av dataskyddsförordningen och övervaka efterlevnaden av den personuppgiftsansvariges strategi för skydd av personuppgifter. Detsamma framgår även av universitetets interna Rutiner för informationssäkerhet, UFV 2017/93, uppdaterad 2021-03-29. Av Integritetsskyddsmyndighetens webbplats framgår: ”Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen” samt att det bl.a. kan innebära att ”samla in information om hur organisationen behandlar personuppgifter”, ”kontrollera att organisationen följer bestämmelser och interna styrdokument” och ”informera och ge råd inom organisationen”.

Detta ger i förlängningen underlag för att förbättra och vidareutveckla arbetet med att skydda personuppgifter samt bedöma var ytterligare stöd behöver sättas in eller vilka andra åtgärder som behöver vidtas.

Granskningen visar att varken uppföljning, övervakning eller kontroll genomförs av att arbetet med personuppgiftsbehandling och dataskydd inom universitetet bedrivs enligt dataskyddsförordningen. Universitetet som personuppgiftsansvarig saknar former för uppföljning av det arbete som utförs och om dataskyddsförordningen är implementerad och tillämpas inom organisationen. Dataskyddsombudet saknar rutiner för övervakning, tillsyn och kontroll av att dataskyddsförordningen och universitetets strategi för skydd av personuppgifter efterlevs. Enligt uppgift arbetar dataskyddsombudet inte med övervakning, trots att det enligt dataskyddsförordningen är en av dataskyddsombudets huvuduppgifter.[32]

Universitetet har inte heller genomfört någon nulägesanalys eller GAP-analys för att skaffa kunskap om i vilken utsträckning dataskyddsförordningen och interna rutiner är implementerade och tillämpas inom institutionerna. Det har inte heller gjorts någon analytiskt genomgång av universitetets registerförteckning, t.ex. i syfte att identifiera systematiska brister eller luckor i anmälningsrutiner i olika delar av organisationen. [33] Inte heller har exempelvis någon enkätundersökning bland personal som hanterar personuppgifter genomförts för att försöka kartlägga eventuella problem/svagheter och inventera behov av stöd och vidareutveckling.

Internrevisionen har efterfrågat dokumentation i syfte att undersöka om uppföljning och övervakning genomförs med systematik och regelbundenhet, samt om det är möjligt att följa uppföljningsresultat till eventuella följdbeslut om åtgärder för att ”stänga gapen” och vidare till uppföljning av om åtgärderna gett effekt i form av ökad regelefterlevnad. Internrevisionen har dock inte kunnat ta del av sådan dokumentation, då uppföljning och övervakning inte uppges genomföras.

Enligt dataskyddsförordningen är övervakning en av dataskyddsombudets primära uppgifter, och i förordningen framhålls särskilt att det är den personuppgiftsansvariga organisationens, d.v.s. universitetets, ansvar att säkerställa dataskyddsombudets ställning, bl.a. genom att tillhandahålla de resurser som krävs för att fullgöra uppgifterna.[34] Flera av de som intervjuats, däribland dataskyddsombudet, universitetsjuristen och deras närmaste chef, akademiombudsmannen, uppger dock att det, inom ramen för dataskyddsombudets tillsynsfunktion, inte finns tid och resurser att ägna åt övervakning, uppföljning, kontroll eller

[32] Bortsett från den inblick i dataskyddsarbetet (och därigenom indirekt övervakning) som dataskyddsombudet får inom ramen för sina informations- och rådgivningsinsatser (vilka dock beskrivs ske reaktivt och efterfrågebaserat utifrån inkomna frågor och aktuella problem, vilket begränsar lägesbilden).

[33] Registerförteckningen visar enligt uppgift från dataskyddsombudet t.ex. att drygt 760 anmälningar om personuppgiftsbehandlingar inkommit sedan dataskyddsförordningens införande i maj 2018 (varav knappt 70 procent av dessa anmäldes vid införandet 2018-19), att ca 20 procent av institutionerna inte lämnat någon anmälan alls sedan förordningen infördes och att fem anmälningar av ”studentbehandlingar” gällande examensarbeten gjorts sedan rutinen infördes i april 2022. Vidare har 12 st kartläggningar av tredjelandsöverföring av personuppgift registrerats i registret och ett tiotal befarade personuppgiftsincidenter har anmälts till dataskyddsombudet sedan införandet 2018, varav en incident efter utredning har rapporterats vidare till tillsynsmyndigheten.

[34] Dataskyddsombudets uppgifter framgår av dataskyddsförordningen artikel 39 samt av information om dataskyddsombud på tillsynsmyndighetens/IMY:s webbplats. Vad avser övervakning kan detta exempelvis ske genom att samla in information om hur organisationen behandlar personuppgifter samt genom tillsyn och att utföra utvärderingar och kontroller. Av dataskyddsförordningen artikel 38 p. 2 framgår att den personuppgiftsansvarige ska stödja dataskyddsombudet i utförandet av dennes uppgifter genom att tillhandahålla de resurser som krävs för att fullgöra uppgifterna.

andra tillsynsuppgifter. Dataskyddsförordningen beskrivs även som relativt nyinförd (trädde ikraft i maj 2018) och universitetets organisation och dataskyddsarbete uppges därför ännu inte ha uppnått en tillräckligt hög mognadsnivå för att följas upp och övervakas.

Internrevisionen ser dock ett behov av att utvärdera hittills genomförda insatser för att undersöka i vilken utsträckning dataskyddsförordningen är implementerad och tillämpas. Internrevisionens bedömning är således att universitetet, som personuppgiftsansvarig, bör etablera former för uppföljning och dataskyddsombudet införa rutiner för övervakning, kontroll och tillsyn, i syfte att skaffa kännedom och utvärdera om dataskyddsförordningen följs och hur dataskyddsarbetet fungerar inom universitetet. Avsaknad av strukturerad och systematisk uppföljning och övervakning kan innebära att systematiska brister i behandling och skydd av enskildas personuppgifter eller behandling i strid med dataskyddsförordningen inte uppmärksammas och åtgärdas.

3.4 Rapportering

Granskningen visar att universitetet saknar rutin för hur dataskyddsarbetet ska återrapporteras. Det finns inte någon etablerad rapporteringsväg eller rutin som säkerställer återkommande och regelbunden rapportering från dataskyddsombudet direkt till högsta förvaltningsnivå (ej till konsistoriet, inte heller till rektor eller universitetsdirektören).

Dataskyddsombudet ska enligt dataskyddsförordningen rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå – enligt uppgift konsistoriet.[35] Konsistoriet och universitetets ledning behöver för att fatta beslut om förbättringsåtgärder, kunskap om hur dataskyddsarbetet fungerar i praktiken och huruvida dataskyddsförordningen och interna rutiner är implementerade och tillämpas. En central aspekt i det systematiska arbete som ska bedrivas för att skydda personuppgifter är därför fungerande rapportering/återkoppling.

Internrevisionen noterar att det vid universitetet saknas rutin för hur dataskyddsarbetet ska återrapporteras. Det finns inte någon etablerad rapporteringsväg för regelbunden rapportering - varken till konsistoriet, rektor eller universitetsdirektör. I händelse av att det skulle vara påkallat har dock dataskyddsombudet fått acceptans av både konsistoriets ordförande och rektor att kontakta dem, även om det inte finns någon etablerad regelbunden rapporteringsrutin. Av intervjuer framgår att dataskyddsombudet har haft möte med konsistoriets ordförande vid ett tillfälle våren 2021, då bland annat rapporteringsväg diskuterades. Förslag till formaliserad rapporteringsväg diskuterades även vid ett möte mellan dataskyddsombudet, rektor och prorektor i maj 2021.[36] Förslaget till rapporteringsväg har dock inte beslutats eller implementerats i praktiken. Av diarieförda mötesanteckningar från det senare mötet framgår även att dataskyddsombudet informerat ledningen om aktuella dataskyddsfrågor och -problem med stor påverkan och risk för allvarliga konsekvenser för Uppsala universitet, bl.a. gällande tredjelandsöverföringar och behandling av personuppgifter vid studentarbeten.[37]

[35] Dataskyddsförordningen artikel 38. Syftet är att hålla högsta förvaltningsnivå informerat om viktiga frågor och händelser. Enligt diarieförda minnesanteckningar från möte med rektor och prorektor 2021-05-24 konstaterades att högsta förvaltningsnivå, i en styrelsemyndighet som Uppsala universitet, är styrelsen, d.v.s. konsistoriet. UU-DsO 2021/62.

[36] Enligt diarieförda minnesanteckningar från möte med rektor och prorektor 2021-05-24. UU-DsO 2021/62.

[37] Minnesanteckningar från mötet Information om dataskyddsfrågor vid Uppsala universitet 2021-05-24. UU-DsO 2021/62.

Dataskyddsombudet har även, i juni 2022, lyft dataskyddsfrågor som bedömts innebära stor risk och ha stor betydelse för regelefterlevnaden av GDPR/dataskyddsförordningen till rektor, i form av en skriftlig rekommendation.[38]

Internrevisionen har som en del av granskningen efterfrågat dokumentation som visar hur framförda frågor har hanterats vidare, t.ex. om särskilda ställningstaganden krävts för ett förbättrat dataskydd inom dessa områden eller om åtgärder beslutats för att begränsa riskerna eller konsekvenserna. Internrevisionen har inte funnit eller kunnat ta del av dokumentation som visar på beslut/agerande eller på ett systematiskt och strukturerat sätt att omhänderta och hantera sådana ärenden och frågor som dataskyddsombudet lyft uppåt i organisationen.

Att det inte finns någon etablerad rapporteringsväg och rutin för hur dataskyddsarbetet ska återrapporteras, innebär att konsistoriet och ledningen riskerar att gå miste om information om aktuella frågor, allvarliga risker, incidenter eller händelser och därmed inte heller ges förutsättning att vidta åtgärder, begränsa risker/konsekvenser eller fatta andra nödvändiga beslut.

4 Sammanfattande bedömning och rekommendationer

Internrevisionen har granskat om universitetets dataskyddsarbete och rutiner för personuppgiftsbehandling är utformade i enlighet med de krav som ställs i dataskyddsförordningen samt med god intern styrning och kontroll. Granskningen har särskilt inriktats på följande områden: ansvar, roller och styrande dokument, kunskap, information och stöd, uppföljning och övervakning samt rapportering.

Granskningen visar att ett omfattande arbete har genomförts sedan förordningens införande för att utveckla arbetssätt och rutiner för hur personuppgifter ska behandlas, anmälas och skyddas inom universitetet och informations- och stödjande insatser har genomförts för att underlätta implementeringen av dataskyddsförordningen inom organisationen.

Universitetet har ett dataskyddsombud och det finns en ytterligare personell resurs – en universitetsjurist – som också arbetar med GDPR tillsammans med dataskyddsombudet. Inom ramen för deras verksamhet har, sedan införandet av dataskyddsförordningen 2018, arbetet inriktats på att skapa arbetssätt och rutiner för hur personuppgifter ska behandlas, anmälas och skyddas inom universitetet samt på att informera, ge råd och utveckla stödmaterial och vägledning för de medarbetare i organisationen som behandlar personuppgifter. Det har bl.a. införts ett elektroniskt anmälningsförfarande för personuppgiftsbehandlingar (vilka hålls i en registerförteckning) och en funktionsepostlåda som ingång för stöd och rådgivning. Vad avser stöd till institutioner och andra delar av organisationen som behandlar personuppgifter, finns utöver dataskyddsombudets stöd och rådgivning, även ett nära samarbete med informationssäkerhetssamordnarnas stödjande verksamhet.

Trots det betydande arbete som hittills genomförts för att implementera dataskyddsförordningen inom universitetets organisation, bedömer internrevisionen att det kvarstår arbete för att uppnå god intern styrning och kontroll och det krävs ytterligare åtgärder

[38] Tre frågor av stor betydelse för regelefterlevnad av GDPR 2022-06-13. UU-DsO 2022/113.

även i förhållande till krav som ställs i dataskyddsförordningen. I relation till dataskyddsförordningen visar granskningen på brister vad gäller att:

- roll- och ansvarsfördelningen mellan dataskyddsombudet och universitetet som personuppgiftsansvarig inte är tillräckligt tydliggjord och separerad i praktiken,
- dataskyddsombudet följaktligen inte kan upprätthålla en oberoende tillsynsroll,
- dataskyddsombudet inte arbetar med övervakning, tillsyn och kontroll av att dataskyddsförordningen följs trots att det är en av dataskyddsombudets huvuduppgifter,
- det saknas en etablerad rutin som säkerställer regelbunden direktrapportering från dataskyddsombudet till högsta förvaltningsnivå.

Därtill visar granskningen att uppföljning, övervakning och kontroll av universitetets dataskyddsarbete inte utförs systematiskt. Det saknas även universitetsövergripande styrdokument som beskriver hur universitetets dataskyddsarbete ska vara organiserat, roll- och ansvarsfördelning, arbetsuppgifter samt rutiner för uppföljning, övervakning och rapportering. Därutöver finns ett behov av förstärkta och målgruppsanpassade informations- och utbildningsinsatser. Internrevisionen noterar att det universitetsgemensamma dataskyddsarbetet i högre grad behöver styras, planeras och genomföras med systematik och struktur.

Internrevisionens sammanfattande bedömning är att ett stort förbättringsbehov föreligger, vad avser de områden där iakttagelser framförts under granskningen, innan universitetets dataskyddsarbete kan anses vara utformat i enlighet med dataskyddsförordningens krav och med god intern styrning och kontroll. Internrevisionen rekommenderar därför rektor att:

- tydliggöra roller, ansvarsfördelning och arbetsuppgifter för dataskyddsombudet och universitetet som personuppgiftsansvarig,
- säkerställa en ändamålsenlig organisering av universitetets dataskyddsarbete, som t.ex. inkluderar en förvaltningsorganisation och en resurs utsedd att arbeta med den personuppgiftsansvariges operativa universitetsgemensamma uppgifter och ärenden,
- upprätta styrande dokument som beskriver hur det universitetsgemensamma dataskyddsarbetet är organiserat, roll- och ansvarsfördelning, vilka arbetsuppgifter som ska utföras av dataskyddsombudet respektive personuppgiftsansvarig, rutiner för uppföljning, övervakning och rapportering,
- säkerställa dataskyddsombudets oberoende ställning och tillsynsroll samt att tillräckliga resurser tillförs ombudet för att utföra uppgifterna som ska utföras enligt dataskyddsförordningen (inklusive övervakning),
- tillse att dataskyddsombudet systematiskt och i god tid involveras i sådana processer där principiella dataskyddsfrågor ofta aktualiseras och kan kräva bedömning och råd utifrån regelefterlevnadsaspekt, t.ex. inför beslut om inköp/upphandling av IT-lösningar,
- säkerställa att medarbetare och studenter som behandlar personuppgifter har tillräckliga kunskaper om dataskyddsförordningen/dataskydd genom förstärkta och målgrupps-anpassade informations- och utbildningsinsatser, t.ex. genom att införa obligatorisk målgruppsanpassad internutbildning samt erbjuda kontinuerliga informationsinsatser,

- införa rutiner för systematisk uppföljning, övervakning och kontroll av att dataskydds-förordningen efterlevs och att interna arbetssätt är implementerade och tillämpas,
- formalisera rapporteringsväg och införa rutin för regelbunden rapportering från dataskyddsombudet till högsta förvaltningsnivå.

Madelene Norsell	Sven Jungerhem
Internrevisor/granskningsledare	Internrevisionschef