Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT

SLU ID: SLU.ua.2026.1.1-1117

Sakområde: 1. Verksamhetsstyrning och organisation samt 11. IT, service, säkerhet och miljö

Dokumenttyp: Regel samt Rutin	Träder i kraft: 2026-04-29
Beslutsfattare: Rektor	Giltighetstid: Tills vidare
Avdelning/kansli: Ledningskansliet	Senast granskad: 2026-04-29
Beslutsdatum: 2026-04-29	Bör granskas före: 2031-04-29

Dokument som upphävs: Molntjänster vid SLU daterat 2017-07-07 och Molntjänster på SLU daterat 2018-01-10 under dnr SLU ua 2017-.1.1.1-2768 samt bilaga till den senare, dnr SLU ua 2018.2.8.2-30

Bilaga till: Rektors beslut om regler och rutin för molntjänster vid SLU

Regler och rutin för molntjänster vid SLU

Molntjänster är en benämning på it-tjänster och resurser – datalagring, beräkningskraft, databaser, nätverk och programvara – som levereras över internet från en leverantörs server och datacenter, snarare än från lokala system eller egna servrar. Det kan till exempel vara lagring, ett enkätverktyg eller programvaror som används on demand och öppnas via en webbläsare.

Den tekniska utvecklingen innebär att allt fler digitala tjänster och program är eller kommer att bli molntjänster. Därför behöver medarbetare vid SLU vara medvetna om vilka regler och rutiner som gäller för molntjänster. Detta dokuments syfte är att klargöra hur molntjänster får anskaffas och användas vid SLU med utgångspunkt i den typ av information som ska behandlas i molntjänsten.

Reglerna och rutinen gäller för samtliga typer av molntjänster, oavsett om de tillhandahålls i ett publikt moln eller ett hybridmoln. Ett **publikt moln** är en it-miljö där servrar, lagring och program hanteras i ett datacenter som ägs av en molntjänstleverantör och delas mellan flera olika kunder via internet. Ett **hybridmoln** är en kombination av ett publikt moln och en egen it-infrastruktur, exempelvis lokala servrar, som integreras med varandra och bildar en sammanhängande it-miljö.

Regler för att anskaffa och använda molntjänster

När en molntjänst anskaffas ska förfarandet följa SLU:s policy för IT-anskaffning.[1]

[1] SLU.ua.2025.1.1-3493 Policy för IT-anskaffning vid SLU.

Innan en molntjänst börja användas måste följande vara uppfyllt:

- Informationen som ska behandlas ska vara informationsklassad.
- Tillämpliga krav i SLU:s kravkatalog för informations- och it-säkerhetskrav ska vara uppfyllda.[2]

Huvudregel

Huvudregeln är att sekretessbelagda uppgifter och känsliga personuppgifter inte får behandlas eller lagras i en molntjänst. Undantag kan göras, men bara om kraven nedan är uppfyllda. System- eller informationsägaren[3] ansvarar för att detta görs.

Sekretessbelagda uppgifter

- Genomföra och dokumentera en lämplighetsbedömning.
- Teckna sekretessavtal med leverantören (om sekretess inte redan regleras i huvudavtalet).

Personuppgifter

- Utreda om personuppgifter kommer att överföras till ett land utanför EU/EES (tredjelandsöverföring).
- Göra en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen (GDPR) om förordningen kräver det.
- Teckna personuppgiftsbiträdesavtal med leverantören.
- Registrera molntjänsten i SLU:s register över personuppgiftsbehandlingar.

Alla ovanstående krav ska vara uppfyllda **innan** några data behandlas i molntjänsten. Övriga säkerhetskrav för molntjänster vid SLU finns i SLU:s kravkatalog för informations- och it-säkerhetskrav[4].

Lämplighetsbedömning när sekretessbelagda uppgifter ska överföras till en molntjänst

Viss information hos SLU omfattas av sekretess. Exempel är hälsouppgifter, anbud vid upphandling samt information om samverkans- och uppdragsforskning.

[2] SLU.ua.2024.1.1.1-1752 Regler för informationsklassning vid Sveriges lantbruksuniversitet. Bilaga 1: Kravkatalog för informations- och it-säkerhetskrav vid Sveriges lantbruksuniversitet.
[3] Se SLU.ua.2023.2.10-2023 Informationssäkerhetspolicy för Sveriges lantbruksuniversitet för information om vem som är systemägare/informationsägare.
[4] SLU.ua.2024.1.1.1-1752 Regler för informationsklassning vid Sveriges lantbruksuniversitet. Bilaga 1: Kravkatalog för informations- och it-säkerhetskrav vid Sveriges lantbruksuniversitet.

Sekretessbelagda uppgifter får överföras till en extern molntjänst bara om leverantören ska tekniskt bearbeta eller tekniskt lagra uppgifterna och om det, med hänsyn till omständigheterna, inte är olämpligt att lämna ut uppgifterna. Detta regleras i 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400).

Innan sekretessuppgifter överförs till en extern molntjänst måste därför en lämplighetsbedömning genomföras. Lämplighetsbedömningen ska ta hänsyn till både molntjänsten och de uppgifter som ska hanteras. Om kraven inte är uppfyllda och sekretessbelagda uppgifter ändå överförs till en extern molntjänst är det ett sekretessbrott.

Lämplighetsbedömningen innehåller flera delar. Nedan beskrivs de två mest centrala, sekretessavtal och tredjelandsöverföring.

Sekretessavtal i lämplighetsbedömningen

Det måste tecknas ett sekretessavtal med leverantören. Sekretessavtalet ska ange att leverantören inte får sprida uppgifterna på något sätt. Ibland finns sekretess-villkoren i huvudavtalet för tjänsten. Om det inte är fallet krävs ett separat sekretessavtal.

Om det inte går att få till ett sekretessavtal med leverantören är molntjänsten i regel inte lämplig att använda.

Tredjelandsöverföring i lämplighetsbedömningen

När SLU behandlar personuppgifter ska behandlingen följa dataskydds-förordningen (GDPR). En personuppgift är en uppgift som direkt eller indirekt kan kopplas till en levande fysisk person, till exempel namn, kontaktuppgifter, IP-adress och löneuppgifter.

En tredjelandsöverföring innebär att personuppgifter överförs till ett land utanför EU/EES. Det kan ske om leverantören har servrar utanför EU/EES, om leverantören ingår i en koncern med bas utanför EU/EES eller om leverantören använder underleverantörer utanför EU/EES.

Om molntjänsten innebär tredjelandsöverföring ska det tas med i lämplighetsbedömningen. Skälet är att länder utanför EU/EES kan ha nationell lagstiftning som ger ett svagare integritetsskydd och som påverkar hur väl sekretessavtalet fungerar i praktiken.

Rutin för lämplighetsbedömning

Informationsägaren, det vill säga prefekten eller motsvarande chef, ansvarar för att en lämplighetsbedömning görs när sekretessbelagda uppgifter ska hanteras i en molntjänst.

Så här gör du en lämplighetsbedömning:

1. Använd mallen *Lämplighetsbedömning av utlämnande av sekretessbelagda uppgifter i it-tjänsten […]*. Du hittar den på dataskydds sida på medarbetarwebben.
2. När bedömningen är klar skickar du den ifyllda mallen till dataskydd@slu.se för att få dataskyddsgruppens rekommendation. Dataskyddsgruppen representerar områdena juridik/dataskydd, informationssäkerhet och it-säkerhet.
3. Dataskyddsgruppen skriver sin rekommendation i bedömningsmallen och skickar tillbaka den till informationsägaren.
4. Informationsägaren beslutar om molntjänsten får användas. Beslutet ska grundas på den samlade bedömningen och dataskyddsgruppens rekommendation. Om flera informationsägare har sekretessbelagda uppgifter i samma molntjänst ska varje informationsägare göra en egen bedömning, eftersom bedömningen kan variera beroende på vilka sekretessbelagda uppgifter som hanteras.
5. Registrera den färdiga lämplighetsbedömningen i Public 360.

Bedömningen kan behöva uppdateras om leverantören av molntjänsten ändrar tjänsten på något sätt. Exempel är ägarbyte, nya inställningar, nya funktioner eller nya samarbetspartners/underleverantörer. Om lämplighetsbedömningen behöver uppdateras, upprepa steg 2–5 ovan.