SUHF

Expertgruppen för
arkiv- och informationshantering

Att ställa arkivkrav på IT-system

- vid universitet och högskolor

SUHF

Expertgruppen för
arkiv- och informationshantering

Att ställa arkivkrav på IT-system, - vid universitet och högskolor
September 2019

Version: 1.0

Utgivare: SUHF:s expertgrupp för arkiv- och informationshantering

Författare: Birgitta Edenius och Margareta Ödmark

SUHF
Expertgruppen för
arkiv- och informationshantering

Innehåll

SUHF
Expertgruppen för
arkiv- och informationshantering

Inledning

Redan innan upphandlingen av ett IT-system[1] startar och en kravspecifikation tas fram behöver lärosätet göra en informationsvärdering för att fastställa om systemet kommer att hantera allmänna handlingar eller inte. Om informationsvärderingen visar att IT-systemet kommer att innehålla allmänna handlingar behöver alltid arkivkrav ställas i varierande omfattning. Arkivkraven leder i sin tur till olika åtgärder, varav vissa kan göras en gång vid systeminförandet medan andra åtgärder behöver genomföras löpande. Även vid vidareutveckling och vid avveckling av IT-system behöver informationsvärderingar göras och arkivkrav ses över.

Informationsvärderingen är också ett sätt att fastställa om IT-systemet kommer att hantera allmänna handlingar endast som ett tillfälligt arbetsredskap utan bevarandekrav på informationen, om det kommer att hantera personuppgifter, eller om det kommer att hantera annan information där hänsyn behöver tas till olika aspekter inom informationssäkerhet.[2]

Riksarkivet har föreskriftsrätt gällande allmänna handlingar och kan därför ställa krav på myndigheternas hantering. Kraven innebär att myndigheterna ska vidta åtgärder så att digitala handlingar fortlöpande kan framställas, överföras, dokumenteras, hanteras, förvaras och vårdas så att de kan presenteras upprepat under den tid som de ska bevaras[3].

Givetvis har verksamheten också ett eget behov av att kunna återsöka och återanvända sin egen information över tiden.

Målgrupp för dokumentet

Dokumentet riktar sig till flera målgrupper med olika kompetenser och kunskapsområden vid lärosätena. De målgrupper som har identifierats är:

- Arkivfunktion
- IT-avdelning inklusive ev. systemförvaltningsgrupper
- Inköps-/upphandlings funktion
- Den verksamhet som har behov av IT-systemet
- Ytterligare kompetenser beroende på IT-systemets funktion och informationsinnehåll, exempelvis jurist, dataskyddsombud och informationssäkerhetskompetens

[1] Se begreppslistan
[2] Se Figur 1: Illustration av livscykel för ett IT-system och dess information, med informationsvärdering, arkivkrav och dokumentation. Sidan 8
[3] Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) - RA-FS 2009:1 4 kap. 1§

SUHF
Expertgruppen för
arkiv- och informationshantering

Syfte med dokumentet

Syftet med detta dokument är att underlätta för lärosätenas olika verksamheter att kunna ställa rätt krav vid upphandlingen av nya IT-system samt vid utveckling och avveckling av befintliga system. Dokumentet ska vara ett stöd för att förstå betydelsen av olika obligatoriska krav och varför det är viktigt att de omhändertas.

Avgränsning

De krav som lyfts fram och beskrivs är generella och gemensamma. Det är de krav som behöver ställas vid en upphandling oavsett vilket IT-system som ska upphandlas. Även vid vidareutveckling och vid avveckling av IT-system behöver informationsvärderingar göras och arkivkrav ses över.

Kraven behöver kompletteras med både lärosätesspecifika krav och med de krav som behöver ställas på ett specifikt IT-system.

Om det finns allmänna handlingar som:

- *ska bevaras* i ett IT-system, så ska systemet ge stöd för arkivering både under drift och vid avveckling
- *inte ska bevaras* i ett IT-system, så ska systemet ge stöd för gallring både under drift och vid avveckling

Varför ställa arkivkrav på IT-system?

Genom att ställa arkivkrav på IT-system ges lärosätet möjligheter att ha en effektiv och kontinuerlig dokumenthantering med god informationskvalité.

För digital information som ska arkiveras finns en internationell standard, OAIS[4], vilken förutsätter att arkivkrav ställs på IT-system för att en arkivering överhuvudtaget ska kunna vara möjlig. Syftet är bl.a. att så kallade arkivpaket (Submission Information Package, SIP) ska kunna skapas av IT-systemet för export och leverans till ett e-arkiv eller till en mellanlagringslösning. OAIS-modellen används brett internationellt och nationellt. Och övrigt regelverk, exempelvis Riksarkivets föreskrifter, utgår från denna standard.

[4] Se begreppslistan

Kostnadseffektivitet

Hantering av digital information genererar kostnader. Förr eller senare uppstår kostnader för att iordningställa informationen, om inte förr så inför leverans till arkivmyndighet. För en bättre kostnadseffektivitet måste arkivkrav ställas på IT-systemet så att följande kostnader kan minimeras:

- Kostnader för licenser och avtal för system som inte kan avvecklas
- Kostnader för förvaltning av passiva system som inte kan avvecklas
- Kostnader för lagring och backuper i system som inte kan avlastas på information
- Kostnader för migrering och konvertering av information från gamla system till nya system
- Kostnader för vidareutveckling av system för att möjliggöra gallring och arkivering – krav i och med GDPR[5]

Informationssäkerhet ur arkivsynpunkt

Digital information ska skyddas så att den inte kommer otillbörlig tillhanda, förstörs eller förvanskas. Informationssäkerhet sträcker sig över ett stort område och har flera aspekter. De krav som tas upp här är de som mer direkt påverkar ur arkivsynpunkt, så fler krav behöver ställas ur andra aspekter av informationssäkerhet. För att uppnå god informationssäkerhet måste den information som IT-systemet kommer att hantera kartläggas och värderas och arkivkrav behöver ställas.

Digital information ska ha följande egenskaper[6] så länge den ska finnas kvar, d.v.s. i vissa fall för all framtid. Egenskaperna måste kunna säkerhetsställas i IT-systemet:

- Autenticitet – det ska vara möjligt att bevisa att informationen är vad den utger sig för att vara och att den har skapats/skickats av en viss person vid den tidpunkt som anges
- Pålitlighet – det ska vara möjligt att lita på att informationens innehåll verkligen speglar vad som hänt, sagts, beslutats etc. och att det är rätt version av informationen
- Integritet – det ska vara möjligt att se att informationen är fullständig och inte har blivit ändrad
- Användbarhet – det ska vara möjligt att återsöka, visa och tolka informationen

Verksamhetsnytta

Att lärosätets egen information kan återsökas och återanvändas ger verksamhetsnytta och underlättar organisationens arbete, nu och i framtiden.

---

[5] Se begreppslistan

[6] ISO 15489-1, Information and documentation - Records management. Svensk och internationell standard för informations- och dokumenthantering.

SUHF
Expertgruppen för
arkiv- och informationshantering

Regeluppfyllnad

Hanteringen av allmänna handlingar samt behandlingen av personuppgifter är regelstyrd. För att uppfylla regelverket måste arkivkrav ställas på IT-system.

Lagkrav:

- Offentlighetsprincipen[7] – för att kunna uppfylla det grundlagsskyddade kravet på allmänhetens rätt till insyn samt för att kunna bevara personuppgifter enligt GDPR:s rättsliga grund *allmänt intresse för arkivändamål.*
- GDPR – för att kunna uppgiftsminimera behandlingen av personuppgifter ska IT-system ha ett inbyggt dataskydd[8] och dataskydd som standard[9]

Internationellt ramverk:

- FAIR-principerna[10] – för att uppfylla principerna som är framtagna för forskningsdata, men som egentligen är ett generellt förhållningssätt till information

Genom att ställa arkivkrav på IT-system ges lärosätet möjligheter att uppnå:

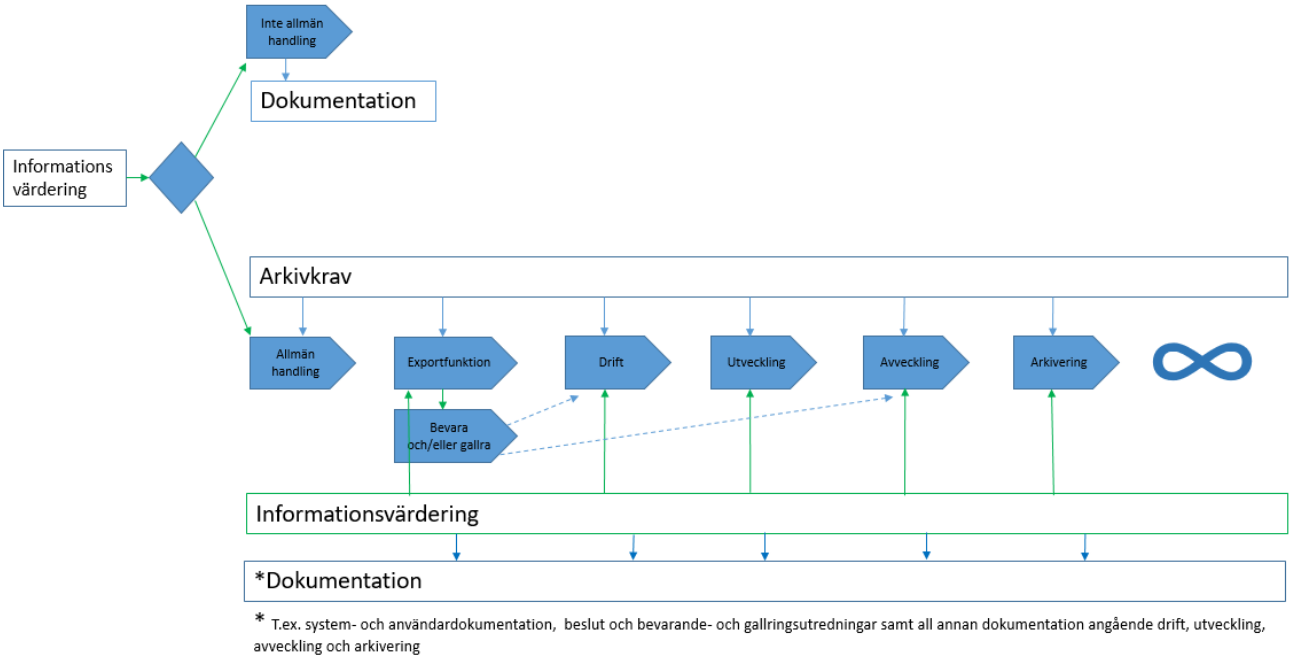
- Kostnadseffektivitet
- Informationssäkerhet ur arkivsynpunkt
- Verksamhetsnytta
- Regeluppfyllnad

[7] Se begreppslistan
[8] Se begreppslistan
[9] Se begreppslistan
[10] Se begreppslistan

SUHF
Expertgruppen för
arkiv- och informationshantering

Övergripande arbetsprocess i text och bild

För att skapa information som uppfyller kraven på autenticitet, pålitlighet, integritet och användbarhet krävs ett antal åtgärder. Vissa åtgärder kan göras en gång och kravställas inför systeminförandet, medan andra behöver genomföras löpande.



Figur 1: Illustration av livscykel för ett IT-system och dess information, med informationsvärdering, arkivkrav och dokumentation.

Bilden (*Figur 1*) illustrerar livscykeln för ett IT-system och dess information, och hur informationsvärderingen och arkivkraven följer systemet hela vägen. Parallellt med detta löper dokumentationen av olika åtgärder och beslut.

1. En initial informationsvärderingen görs för att ta reda på om IT-systemet innehåller allmänna handlingar eller inte. Systemet kan också vid informationsvärderingen visa sig vara ett arbetsverktyg som kommer att hantera allmänna handlingar, men som ingen information ska bevaras ifrån
2. Även om informationsvärderingen visar att systemet inte innehåller allmänna handlingar eller att det är ett arbetsverktyg enligt beskrivningen ovan, kan det innehålla personuppgifter eller annan information som behöver hanteras ur GDPR- eller annat informationssäkerhets perspektiv

3. Informationsvärdering görs kontinuerligt under IT-systemets livscykel om systemet innehåller allmänna handlingar som ska bevaras och arkivkrav hanteras löpande. Alla beslut av vikt dokumenteras

- Informationen ska kunna läsas och förstås under hela dess livscykel
- Lärosätena ska kontinuerligt värdera sin information för att bedöma om den ska bevaras eller gallras

Så här förhåller sig Arkivlagen och GDPR till varandra

GDPR är en EU-förordning och det innebär att den är direkt tillämpbar på alla medlemsländer. GDPR lämnar dock möjlighet för nationella bestämmelser att komplettera i vissa frågor. För Sveriges del innebär denna möjlighet att vi inom offentlighetsrätten har en nationell lagstiftning som getts tolkningsföreträde före GDPR.

Bestämmelserna i Tryckfrihetsförordningen och Arkivlagen går som en följd av detta före bestämmelserna i GDPR när det gäller bevarande och gallring av personuppgifter i allmänna handlingar. Det är en missuppfattning att myndigheter som omfattas av offentlighetsprincipen måste radera personuppgifter när de inte längre behövs. Enligt Arkivlagen ska uppgifterna bevaras, om det inte finns ett godkänt beslut om gallring[11], även om huvudregeln i GDPR säger annorlunda.

Den svenska Dataskyddslagen säger också att myndigheters insamlade personuppgifter får lagras under en längre tid än vad som normalt gäller, om uppgifterna kommer att behandlas för *arkivändamål av allmänt intresse*. Detta är nödvändigt för att den svenska grundlagsskyddade offentlighetsprincipen ska kunna fungera. Men detta kräver i sin tur att IT-systemet anpassas till denna hantering, och här är informationsvärdering samt hantering av arkivkrav en nyckel till att åstadkomma denna anpassning.

[11] Ett gallringsbeslut måste alltid ha stöd i Riksarkivets föreskrifter eller i myndigheternas tillämpningsbeslut av Riksarkivets föreskrifter.

SUHF
Expertgruppen för
arkiv- och informationshantering

Arkivkrav

Systemet ska ha en exportfunktion

- *för att det ska vara möjligt att flytta information som ska bevaras ur systemet*

Att en exportfunktion ska finnas är grunden för att ett bevarande ska vara möjligt, och det kan tyckas vara en självklarhet att detta finns och att det fungerar. Export av information kan också behöva göras mellan olika verksamhetssystem innan informationen arkiveras i ett senare skede. I och med kravet om exportfunktion läggs en grund som sedan arkivkraven under följande rubriker förfinar och specificerar ytterligare.

Om IT-systemet innehåller allmänna handlingar som ska bevaras så kravställ redan från början att en exportfunktion finns som möjliggör att information kan flyttas ut ur systemet för att kunna levereras till ett e-arkiv. I vissa fall är det till och med lämpligt att upprätta anslutningen till e-arkivet samtidigt som systemet införs. Planera för vilken information som ska ingå i arkivuttagen, hur den ska struktureras och med vilka intervaller leveranser ska ske. Upprätta strategier och bevarandeplaner för att kunna föra över informationen och möjliggöra ett bevarande.

För att lärosätena ska kunna tillgodose allmänhetens rätt till insyn får allmänna handlingar som innehåller personuppgifter arkiveras digitalt. Detta baseras på den rättsliga grunden *allmänt intresse för arkivändamål*. Information som tidigare samlats in och behandlats med stöd av en tidsbegränsad rättslig grund enligt GDPR måste för att få bevaras kunna exporteras ur befintligt IT-system och e-arkiveras. IT-systemet behöver således även ur ett arkivperspektiv ha inbyggt dataskydd och dataskydd som standard.

Så länge information är lagrad i ett system är det programvaran som upprätthåller informationens struktur och samband. Denna struktur måste kunna upprätthållas även när informationen lämnar systemet. En export måste kunna göras så att befintliga systemberoende länkar och id-begrepp kan översättas till eller kompletteras med systemoberoende sådana.

Systemet ska kunna exportera information:

- för digital arkivering
- för uttag även under drift

Kravbeskrivning	**Författning**
Teknisk funktion för export av information ska finnas i IT-systemet	
Vid export ska struktur och samband kunna upprätthållas och sammanställningsmöjligheterna inte förvanskas eller försvinna	RA-FS 2009:1

Systemet ska uppfylla krav på informationskvalitet och skydd av informationen

- f*ör att det ska vara möjligt att framställa och presentera handlingar under den tid som de ska bevaras*
- *för att det ska vara möjligt att kunna spåra förändringar*

Vanligt förekommande och/eller leverantörsoberoende filformat rekommenderas för att minska risken för att data förloras vid konvertering eller inte går att läsa då rätt version av programvara saknas. Möjligheten att bevara digital information ökar också om lärosätet redan från början väljer att lagra informationen i enkla och stabila filformat. Om det inte är möjligt, eller om bevarandeformaten innebär alltför stor förlust av funktionalitet, bör lärosätet senast vid publicering eller utskick konvertera till ett godkänt format. Observera att senast vid ett uttag för arkivering ska filformatet alltid konverteras till ett godkänt bevarandeformat. För viss typ av information, exempelvis geografisk information, ljud och rörlig bild, finns i dagsläget inga godkända bevarandeformat. Det bästa alternativet är då att välja att lagra informationen i etablerade standardformat, och en dialog bör då föras med lärosätets arkivfunktion samt övriga informationshanteringsfunktioner, exempelvis lärosätets DAU-funktion eller motsvarande.

IT-systemet behöver använda en godkänd teckenuppsättning för att möjliggöra att informationen går att läsa över tid, men också för att olika programvaror ska tolka och presentera informationen lika.

I systemet ska en enhetlig och definierad vokabulär användas för att möjliggöra att informationen kan bevaras eller migreras till ett nytt system. Med enhetlig och definierad vokabulär avses exempelvis lista med förvalda begrepp eller värden, exempelvis så att personnummer och datum bara kan skrivas på ett sätt. Detta gör det lättare att migrera informationen till andra IT-system och att arkivera den.

En logg är en förteckning över händelser som är noterade i den ordning de inträffar. Vilka händelser som loggas bestäms delvis av operativsystemet, men behöver också kravställas vid upphandling så att verksamhetens behov och krav uppfylls. De flesta loggar är för att drift och förvaltning ska kunna finna orsaken till uppkomna fel, men det finns även loggar över vad som ändras, vem som gjort ändringen och när ändringen är gjord. De flesta loggar får gallras[12], men vissa loggar måste bevaras eller vara kvar en viss tid för att informationen som är allmänna handlingar ska kunna förstås. Detta är viktigt inte minst för att uppfylla Arkivlagens krav på ett bevarande för rättsskipningens behov.

Kravet på att IT-system ska logga händelser är starkt knutet till informationssäkerhetens krav ur arkivsynpunkt på att digital information ska vara autentisk, pålitlig, ha integritet och vara användbar.

[12] Se begreppslistan

SUHF
Expertgruppen för
arkiv- och informationshantering

Systemet :
- bör under drift använda ett godkänt bevarandeformat
- ska senast vid uttag för arkivering kunna konvertera filer till ett godkänt bevarandeformat
- bör senast vid publicering eller utskick konvertera filer till ett godkänt bevarandeformat
- ska använda en godkänd teckenuppsättning för att möjliggöra läsbarhet över tid
- ska använda en enhetlig och definierad vokabulär
- ska kunna presentera och bevara loggar

Kravbeskrivning	**Författning**
Systemet ska senast vid uttag för arkiv konvertera filer till ett godkänt bevarandeformat	RA-FS 2009:1, RA-FS 2009:2
Systemet bör senast vid publicering/distribuering konvertera filer till ett godkänt bevarandeformat	
För information som ska gallras ska sådant filformat användas som möjliggör att informationen går att läsa och förstå fram till dess att den gallras	
Val av filformat, om och när konvertering av filformat ska ske, ska anges i systemdokumentationen	RA-FS 2009:1
Om elektroniska signaturer förekommer ska de uppfylla Riksarkivets krav på format	RA-FS 2009:2
Teckenuppsättning som uppfyller Riksarkivets krav ska användas i systemet, och ska anges i systemdokumentationen	RA-FS 2009:1 RA-FS 2009:2
En enhetlig och definierad vokabulär ska användas för digitala handlingar som ska bevaras eller som har en lång gallringsfrist	RA-FS 2009:1
IT-systemet ska kunna logga händelser	
Loggar ska vara självförklarande, d.v.s. vara oberoende av systemets information för att kunna läsas och förstås	

Systemet ska kunna särskilja information med olika status

- *för att det ska vara möjligt att söka fram, lämna ut och återanvända digitala handlingar*

I systemet ska det utan problem vara möjligt att kunna skilja allmänna handlingar från arbetshandlingar, exempelvis utkast. Sekretessbelagd information ska kunna skyddas utan att insynen försvåras i de handlingar som är offentliga. Detta ställer krav på att sekretessbelagd information märks upp med metadata. I vissa system kan det även finnas behov av att märka upp handlingar med vilken paragraf i Offentlighets- och sekretesslagen som verksamheten hänvisar till. Det gäller framförallt system där det finns behov av att kunna sätta olika behörigheter. Även information som inte är sekretessbelagd enligt Offentlighets- och sekretesslagen kan behöva särskiljas, metadatasättas och skyddas utifrån exempelvis regelverket kring behandling av personuppgifter.

Om informationen inte omfattas av ett gallringsbeslut bör det vara möjligt att återskapa hur en allmän handling sett ut vid en given tidpunkt. Har informationen ändrats eller tillförts handlingen ska det då framgå att detta har skett och när.

Handlingar som hör till ett ärende ska i möjligaste mån presenteras samlat så att det är lätt att följa ärendets gång. Handlingar i ett ärende- och dokumenthanteringssystem ska exempelvis förses med metadata som gör att det kan förstås vilket ärende de hör till.

Systemet ska kunna:

- skilja arbetshandlingar från allmänna handlingar
- skilja offentliga handlingar från handlingar med sekretess
- skilja på handlingar med olika sekretess
- versionshantera handlingar

Kravbeskrivning	**Författning**
Handlingar i systemet ska vara möjliga att presentera, läsa och förstå under hela sin livscykel	RA-FS 2009:1
Om systemet innehåller allmänna handlingar ska de vara möjliga att lämna ut i pappers- eller digitalt format	TF (1949:105) OSL (2009:400) RA-FS 2009:1
Stöd för versionshantering bör finnas i systemet	RA-FS 2009:1
För handlingar som ska bevaras gäller att systemet ska kunna säkerställa ett bevarande av den ursprungliga handlingen innan ändring görs	RA-FS 2009:1

Systemet ska ha en gallringsfunktion

- *för att det ska vara möjligt att gallra information som bedömts inte ska bevaras*

För att få en effektiv och kostnadsmedveten informationsförsörjning vid lärosätena måste verksamheten kontinuerligt värdera informationens betydelse. Gallring är dock framförallt ett sätt att göra arkiven mer överskådliga och på så sätt också mer lättillgängliga. Det är ovanligt att all information i ett system ska bevaras för all framtid. Redan vid planeringen av ett nytt system ska lärosätet därför analysera vilken information som ska bevaras och vilken som ska gallras. I vissa system ska kanske ingen information bevaras. Personuppgifter ska enligt GDPR inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det medför att det måste vara möjligt att, utan svårigheter, gallra information också när systemet är i drift. Även annan information kan behöva gallras under tiden som systemet är drift. Därför ska det vara möjligt att sätta upp gallringsregler i systemet för vilken information som ska gallras och när det ska ske.

Den bevarande- och gallringsutredning som bör göras vid planeringen av ett nytt system ska kontinuerligt uppdateras under systemets livscykel för att kunna ta hänsyn till ändrade krav från omvärlden och verksamhetens behov. För att få lov att gallra en allmän handling måste det finnas stöd för det i regelverket.

Det är sällan all information ska eller ens får bevaras. Därför ska det i systemet vara möjligt att:

- gallra under drift
- gallra för att uppfylla kravet på uppgiftsminimering enligt GDPR
- sätta upp gallringsregler
- gallra när systemet avvecklas

Kravbeskrivning	**Författning**
Teknisk funktion för gallring bör finnas i systemet	
Om gallring ska utföras i systemet ska det ske i enlighet fastställda gallringsfrister	
Finns gallringsfunktion i systemet, ska resultatet av begärd gallring kunna kontrolleras innan den utförs, för att undvika felaktig gallring	RA-FS 2009:1
I systemet ska det vara möjligt att skilja på information som ska bevaras från gallringsbar information	RA-FS 2009:1
I systemet ska det vara möjligt att skilja på information med olika gallringsfrister	RA-FS 2009:1
Gallringsrapport ska kunna skapas i systemet och den ska minst bestå av: - tidpunkt för gallring - vem som utfört gallringen (inte vid automatiserad gallring) - vad som gallrats	
Gallrad information ska inte kunna återskapas	

SUHF
Expertgruppen för
arkiv- och informationshantering

Systemet ska kunna knyta metadata till informationen

- *för att det ska vara möjligt att över tid förstå, hantera och återsöka information*

Metadata är data som beskriver informationens sammanhang, innehåll och struktur. Den beskriver även hur informationen ska hanteras över tid. Metadata gör det möjligt att söka information på ett strukturerat sätt och bedöma om informationen är tillförlitlig.

Det finns olika typer av metadata och dessa fyller olika syften.

- Metadata som sätter in informationen i ett sammanhang, exempelvis vem som skapat informationen i vilket system och till vilket verksamhetsområde och process den hör
- Metadata som gör det lättare för den egna verksamheten och andra intressenter att söka och återanvända informationen, exempelvis diarienummer och andra unika beteckningar
- Metadata som beskriver tekniska format, exempelvis namn och version av den mjukvara som använts för att skapa informationen samt vilket filformat
- Metadata som beskriver hur informationen ska hanteras, exempelvis om informationen omfattas av sekretess och i så fall enligt vilken paragraf i Offentlighets- och sekretesslagen eller om informationen innehåller personuppgifter

Metadata är viktig och fyller flera olika funktioner. Den behövs för att:

- kunna särskilja, men också hålla samman information
- förstå information över tid
- koder och förkortningar ska förstås över tid
- informationen ska gå att återsöka
- olika system ska vara kompatibla med varandra (Interoperabilitet)

Kravbeskrivning	**Författning**
I systemet ska det finnas möjlighet att metadatasätta informationen i enlighet med den informationsvärdering som gjorts	
Det ska genom metadata vara möjligt att särskilja handlingar som exempelvis - allmänna handlingar från arbetshandlingar - sekretessbelagda handlingar från offentliga handlingar - olika organisationsdelars handlingar från varandra i gemensamma system - handlingar som ska bevaras från handlingar som ska gallras - handlingar med olika gallringsfrister	OSL (2009:400) RA-FS 2009:1
Handlingar som hör till ett ärende ska genom metadata kunna presenteras samlat	
Filer och objekt ska ha unika beteckningar	RA-FS 2009:1

Systemet ska dokumenteras

- *för att säkerhetsställa att informationen kan förstås och presenteras upprepat under den tid som den ska bevaras*

Lärosätet ska ha en fastställd strategi för bevarande i vilket det framgår vilka åtgärder som lärosätet avser att vidta för att säkerställa ett bevarande av digitala allmänna handlingar[13]. Lärosätet ska dokumentera sina digitala handlingar för att handlingarna ska kunna framställas, överföras, hanteras, förvaras och vårdas på ett tillfredsställande sätt under den tid som de ska bevaras. Dokumentationen ska även hjälpa framtidens användare att tolka informationen och förstå i vilket sammanhang den skapades.

Dokumentation om systemet består av system- och användardokumentation[14]. När ett system tas i drift finns i de flesta fall dokument som beskriver hur systemet är uppbyggt. Den dokumentationen kompletteras sedan med information om hur systemet använts över tid och förvaltas på lärosätet. Dokumentationen om systemet ska kompletteras och uppdateras under systemets hela livscykel.

Dokumentationen bör kompletteras med en bevarande- och gallringsutredning av systemet som innehåller en informationsbeskrivning och en informationsvärdering. Här kan också den digitala informationen i systemet beskrivas i relation till eventuella kompletterande handlingar på papper eller i annan format utanför systemet. Utredningen ligger till grund för, och kompletterar, den bevarandeplan som behöver upprättas för systemets drift och förvaltning. En bevarande- och gallringsutredning bör göras innan systemet tas i drift och kompletteras vid större förändringar samt vid avveckling. Den är ett redskap för en kontinuerlig informationsvärdering och ger möjlighet att ställa rätt krav vid upphandling, utveckling och avveckling.

Dokumentation ska finnas över systemet så att dess digitala handlingar kan framställas, hanteras och tolkas på ett korrekt sätt under hela den tid de ska bevaras

[13] RA-FS 2009:1

[14] Se även Riksarkivets: *Radgivning_systemdokumentation_ver0.84 (PDF tillgänglig på Riksarkivets webbplats) - Råd om hur bestämmelserna i RA-FS 2009:1, 5 kap 4-6 §§ ska tolkas och tillämpas – Dokumentationen av elektroniska handlingar*

SUHF
Expertgruppen för
arkiv- och informationshantering

Kravbeskrivning	Författning
Dokumentation ska finnas över systemet så att dess digitala handlingar kan framställas och hanteras på ett korrekt sätt även efter att den överförts till e-arkiv. Dokumentationens omfattning och innehåll kan variera. Om systemet innehåller information som ska bevaras ska dokumentationen minst innehålla följande: - översiktlig beskrivning av systemet och dess digitala handlingar - redogörelse för informationsinnehållet - redogörelse för registrerings- och uttagsmöjligheter - beskrivning av relationer – mellan system och mellan moduler inom systemet - beskrivning över hur koder och förkortningar har använts och vad de betyder - beskrivning av rutiner och funktioner - beskrivning av struktur och samband för lagrade data - redogörelse för informationskvalitet - redogörelse för användningen av standarder samt i förekommande fall avvikelser från standarder - redogörelse för relationen till lärosätets strategi för bevarande - dokumentation av test och utvärdering vid driftsättning och utveckling - dokumentation rörande informationssäkerhet - dokumentation rörande den gallring som sker av digitala handlingar	RA-FS 2009:1
Dokumentationen över systemet ska hållas aktuell, kunna återsökas och kunna presenteras samlat samt versionshanteras	RA-FS 2009:1
Dokumentation i digitalt format ska senast vid arkivuttag konverteras till bevarandeformat	
Planerad export ska anges i drifts- och förvaltningsplan	RA-FS 2009:1
Om godkända filformat inte används från början ska plan för konvertering finnas och vara dokumenterad så att de digitala handlingarna går att läsa och förstå under den tid de ska bevaras	RA-FS 2009:1, RA-FS 2009:2
Ange i dokumentation om elektroniska signaturer förekommer, vid vilka tillfällen (exempelvis inkomna eller utgående skrivelser), och i vilket format	RA-FS 2009:1

SUHF
Expertgruppen för
arkiv- och informationshantering

Begreppslista

Begrepp	Förklaring	Källa/referens
Allmän handling	Med handling förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. En handling är allmän, om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos myndigheten.	Tryckfrihetsförordningen 2 kap. 3-4 §
Dataskydd som standard (se även *inbyggt dataskydd*)	(engelska privacy by default) Del av GDPR som i korthet innebär att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i ett IT-system är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. Detta ställer i sin tur krav på tekniska och organisatoriska åtgärder	(EU) 2016/679
DAU (Data Access Unit)	En DAU är en lokal funktion på lärosätet som erbjuder stöd till forskare i frågor som rör tillgängliggörandet och bevarandet av forskningsdata i enlighet med FAIR-principerna. DAU är den vanligaste benämningen men funktionen kan ha olika benämningar på olika lärosäten, exempelvis DCU (Digital Curation Unit)	
FAIR-principerna	(Findable, Accessible, Interoperable, Reusable) FAIR-principerna är ett internationellt erkänt ramverk som är framtaget för forskningsdata. Men det innebär egentligen ett generellt förhållningssätt till information. Principerna pekar på de fyra ovan nämnda egenskaperna som information ska inneha	
Gallring	Gallring innebär att informationen raderas eller förstörs. Gallrad information ska inte gå att återskapa. Riksarkivets definition av gallring är: Förstöra allmänna handlingar eller uppgifter i allmänna handlingar, eller vidta andra åtgärder med handlingarna som medför – förlust av betydelsebärande data, – förlust av möjliga sammanställningar, – förlust av sökmöjligheter, eller	RA-FS 1991:1, med ändringar och omtryck

	– förlust av möjligheter att bedöma handlingarnas autenticitet	
Gallringsfrist	Den tid som ska förflyta innan en allmän handling får gallras enligt gallringsbeslut	
GDPR (General Data Protection Regulation)	(svenska Dataskyddsförordningen) Förordningen är en del i regelverket för att skydda enskildas grundläggande rättigheter och friheter, och särskilt deras rätt till skydd av personuppgifter	(EU) 2016/679
Inbyggt dataskydd (se även *dataskydd som standard*)	(engelska privacy by design) Del av GDPR som innebär att hänsyn ska tas till integritetsskyddsreglerna redan när IT-system och rutiner utformas. Det är ett sätt att se till att kraven i GDPR uppfylls och att den registrerades rättigheter skyddas. Detta ställer i sin tur krav på tekniska och organisatoriska åtgärder	(EU) 2016/679
IT-system	I dokumentet har begreppet IT-system använts. Med detta begrepp inkluderas vad som i vissa fall även benämns IT-tjänster, vilka i sin tur kan vara molnbaserade eller på annat sätt externa. Det är informationen och ägarskapet till informationen som är i fokus och som gör att arkivkrav behöver ställas på den tekniska lösningen.	
OAIS (Open Archival Information System)	En internationell ISO-standard som är ett ramverk för elektroniska arkiv (e-arkiv). Modellen är ursprungligen utvecklad av NASA för att hantera och lagra digital information.	ISO 14721
Offentlighetsprincipen	Offentlighetsprincipen handlar om att ge allmänheten insyn i offentliga verksamheter. Principen kommer till uttryck på flera sätt i svensk lag bl.a. i Tryckfrihetsförordningen, Offentlighets- och sekretesslagen och Arkivlagen	

SUHF
Expertgruppen för
arkiv- och informationshantering

Relevant regelverk

- Arkivlagen (1990:782)

- Dataskyddsförordningen/GDPR (General Data Protection Regulation) (EU) 2016/679. Europaparlamentets och rådets förordning av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

- Dataskyddslagen (2018:218)

- Offentlighets- och sekretesslagen (2009:400, OSL)

- Riksarkivets föreskrifter och allmänna råd (RA-FS samt RA-MS), främst:
    - RA-FS 2009:1, Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling)
    - RA-FS 2009:2, Riksarkivets föreskrifter och allmänna råd om tekniska krav för elektroniska handlingar (upptagningar för automatiserad behandling)

- Riksarkivets förvaltningsgemensamma specifikationer (FGS)

- Tryckfrihetsförordningen (1949:105)

SUHF
Expertgruppen för
arkiv- och informationshantering

Bilaga 1, Sammanställning av arkivkrav

Systemet ska ha en exportfunktion
Teknisk funktion för export av information ska finnas i IT-systemet
Vid export ska struktur och samband kunna upprätthållas och sammanställningsmöjligheterna inte förvanskas eller försvinna

Systemet ska uppfylla krav på informationskvalitet och skydd av informationen
Systemet ska senast vid uttag för arkiv konvertera filer till ett godkänt bevarandeformat
Systemet bör senast vid publicering/distribuering konvertera filer till ett godkänt bevarandeformat
För information som ska gallras ska sådant filformat användas som möjliggör att informationen går att läsa och förstå fram till dess att den gallras
Val av filformat, om och när konvertering av filformat ska ske, ska anges i systemdokumentationen
Om elektroniska signaturer förekommer ska de uppfylla Riksarkivets krav på format
Teckenuppsättning som uppfyller Riksarkivets krav ska användas i systemet, och ska anges i systemdokumentationen
En enhetlig och definierad vokabulär ska användas för digitala handlingar som ska bevaras eller som har en lång gallringsfrist
IT-systemet ska kunna logga händelser
Loggar ska vara självförklarande, d.v.s. vara oberoende av systemets information för att kunna läsas och förstås

Systemet ska kunna särskilja information med olika status
Handlingar i systemet ska vara möjliga att presentera, läsa och förstå under hela sin livscykel
Om systemet innehåller allmänna handlingar ska de vara möjliga att lämna ut i pappers- eller digitalt format
Stöd för versionshantering bör finnas i systemet
För handlingar som ska bevaras gäller att systemet ska kunna säkerställa ett bevarande av den ursprungliga handlingen innan ändring görs

Systemet ska ha en gallringsfunktion
Teknisk funktion för gallring bör finnas i systemet
Om gallring ska utföras i systemet ska det ske i enlighet fastställda gallringsfrister
Finns gallringsfunktion i systemet, ska resultatet av begärd gallring kunna kontrolleras innan den utförs, för att undvika felaktig gallring
I systemet ska det vara möjligt att skilja på information som ska bevaras från gallringsbar information
I systemet ska det vara möjligt att skilja på information med olika gallringsfrister
Gallringsrapport ska kunna skapas i systemet och den ska minst bestå av: - tidpunkt för gallring - vem som utfört gallringen (inte vid automatiserad gallring) - vad som gallrats
Gallrad information ska inte kunna återskapas

Systemet ska kunna knyta metadata till informationen
I systemet ska det finnas möjlighet att metadatasätta informationen i enlighet med den informationsvärdering som gjorts
Det ska genom metadata vara möjligt att särskilja handlingar som exempelvis: - allmänna handlingar från arbetshandlingar - sekretessbelagda handlingar från offentliga handlingar - olika organisationsdelars handlingar från varandra i gemensamma system - handlingar som ska bevaras från handlingar som ska gallras - handlingar med olika gallringsfrister
Handlingar som hör till ett ärende ska genom metadata kunna presenteras samlat
Filer och objekt ska ha unika beteckningar

Systemet ska dokumenteras
Dokumentation ska finnas över systemet så att dess digitala handlingar kan framställas och hanteras på ett korrekt sätt även efter att den överförts till e-arkiv. Dokumentationens omfattning och innehåll kan variera. Om systemet innehåller information som ska bevaras ska dokumentationen minst innehålla följande: - en översiktlig beskrivning av systemet och dess digitala handlingar - en beskrivning av informationsinnehållet - en redogörelse för registrerings- och uttagsmöjligheter - en beskrivning av relationer – mellan system och mellan moduler inom systemet - en beskrivning över hur koder och förkortningar har använts och vad de betyder - en beskrivning av rutiner och funktioner - en beskrivning av struktur och samband för lagrade data - en redogörelse för informationskvalitet - en redogörelse för användningen av standarder samt i förekommande fall avvikelser från standarder - en redogörelse för relationen till lärosätets strategi för bevarande - en dokumentation av test och utvärdering vid driftsättning och utveckling - en dokumentation rörande informationssäkerhet - en dokumentation rörande den gallring som sker av digitala handlingar

Dokumentationen över systemet ska hållas aktuell, kunna återsökas och kunna presenteras samlat samt versionshanteras
Dokumentation i digitalt format ska senast vid arkivuttag konverteras till bevarandeformat
Planerad export ska anges i drifts- och förvaltningsplan
Om godkända filformat inte används från början ska plan för konvertering finnas och vara dokumenterad så att de digitala handlingarna går att läsa och förstå under den tid de ska bevaras
Ange i dokumentation om elektroniska signaturer förekommer, vid vilka tillfällen (exempelvis inkomna eller utgående skrivelser), och i vilket format

SUHF
Expertgruppen för
arkiv- och informationshantering

Bilaga 2, Bevarande- och gallringutredning. Förslag till mall

Denna mall kan användas som ett stöd vid genomförandet av en bevarande- och gallringsutredning.

Se separat mall i Word-format.