UNINETT Fagspesifikasjon

# Retningslinjer for klassifisering av INFORMASJON

| | |
|---|---|
| UFS nr: | 136 |
| Status: | Godkjent |
| Dato: | 21.06.2013 |
| Arbeidsgruppe: | Informasjonssikkerhet |
| Ansvarlig: | Øivind Høiem |
| Kategori: | Anbefaling |

## Sammendrag

Dette dokumentet spesifiserer UH-sektorens anbefalte krav til klassifisering av informasjon. Retningslinjene beskriver hvordan man kan identifisere virksomhetens informasjonsobjekter, klassifisere disse med hensyn til sensitivitet og kritikalitet og å definere oppbevaringsperioder og disponeringsregler. Det er spesielt viktig å få gjort denne type klassifisering før man legger informasjon ut i "skyen", og ved bruk av mobile enheter som lesebrett og smarttelefoner.

Retningslinjene har også eksempler på hvordan informasjonsobjekter som er hyppig brukt i sektoren kan klassifiseres og har referanser til relevante standarder, lover og forskrifter.

Videre er dette dokumentet ment som et verktøy for informasjonseiere for å sikre at virksomhetskritisk innhold blir behandlet på rett måte.

## Innholdsfortegnelse

## 1 Innledning

Hensikten med retningslinjene er å beskrive hvordan man kan identifisere virksomhetens informasjonsobjekter, klassifisere disse med hensyn til sensitivitet og kritikalitet og å definere oppbevaringsperioder og disponeringsregler.

Dokumentet er ment som et verktøy for informasjonseiere og andre for å sikre at virksomhetskritisk innhold vil bli tatt vare på, behandlet og avhendet i samsvar med interne og eksterne krav og beste praksis. Det er spesielt viktig å få gjort denne type klassifisering før man legger informasjon ut i "skyen", og ved bruk av mobile enheter som lesebrett og smarttelefoner.

Kapittel 2 gir en oversikt over prosessen for informasjonsklassifisering og gjør rede for attributtene som bør vurderes. Retningslinjene har i vedlegg 1 eksempler på hvordan informasjonsobjekter som er hyppig brukt i universitets- og høyskolesektoren kan klassifiseres.

Vedlegg 2 forklarer skillet mellom et arkiv, bibliotek og en samling som definert i norske arkivstandard (Noark).

En bevarings- og kassasjonsplan er viktig for god drift av et effektivt informasjons-behandlingssystem. Det gir retningslinjer for oppbevaring og disponering av informasjon som genereres i løpet av den daglige virksomhet og sikrer kontinuitet, beskytter organisasjonens juridiske rettigheter, og gjør at informasjonen lett kan hentes fram etter behov. Se vedlegg 3 for mere informasjon.

Retningslinjenes vedlegg 4 beskriver hvordan åpne data i offentlig sektor bør gjøres tilgjengelig.

I vedlegg 5 er det samlet en oversikt med lenker til standarder, lover og forskrifter som institusjonene må forholde seg til i klassifiseringsarbeidet.

Enkelte av klassifiseringene som sikkerhetsklassifisering, sikkerhetsbehov, maksimum nedetid og bevaringsverdi bør basere seg på en risiko- og sårbarhetsvurdering (ROS) og/eller en virksomhetskritikalitetsvurdering (BIA – Business Impact Assessment). UH-sektorens sekretariat for informasjonssikkerhet ved UNINETT kan bistå med slike vurderinger.

Retningslinjene er utarbeidet av UH-sektorens sekretariat for informasjonssikkerhet ved UNINETT i samarbeid med sektoren.

## 2 Informasjonsklassifisering

Når man skal klassifisere informasjonen, kan man bruke en tabell som denne. Kolonnene i tabellen er beskrevet nedenfor. Eksempler på klassifisering finnes i vedlegg 1.

| Eier | Innhold | Hjemmel | Lagrings-sted | Åpne data? J/N | Sikkerhets-klassifisering | Sikkerhets-behov | Maks. nedetid | Bevarings -verdi | Person-oppl.? | Arkiv-nøkkel | Oppbev.-periode | Avhending |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

### Kolonnebeskrivelser:

**Eier**
Hvilken organisatorisk enhet eller prosess har eierskapet til informasjonen.

**Innhold**
Type informasjon, uavhengig av format og medium. Hva informasjonen handler om.

**Hjemmel**
Referanse til regulatoriske dokument (lov, regel, forskrift, styrende dokument) hvor oppbevaring og/eller disponering framgår. For eksempel **offl. § 25** (LOV 2006-05-19 nr 16: Lov om rett til innsyn i dokument i offentleg verksemd, offentleglova § 25) eller **fvl. § 13.1** (LOV 1967-02-10 nr 00: Lov om behandlingsmåten i forvaltningssaker, forvaltningsloven § 13, første ledd).

**Lagringssted**
Navnet på systemet (eks. NOARK-system, annen elektronisk journal, saksbehandlingssystem, økonomisystem m.fl.) og/eller fysiske arkiv der informasjonsobjektet oppbevares i lagringsperioden.

**Åpne data?**
Fornyings-, administrasjons- og kirkedepartementet (FAD) og Direktoratet for forvaltning og IKT (Difi) ønsker å legge forholdene til rette for at offentlige virksomheter skal dele sine data slik at de kan brukes i nye sammenhenger og til nye tjenester. For å sikre at data blir gjort tilgjengelige på en hensiktsmessig måte, bør offentlige virksomheter følge FADs retningslinjer. Se vedlegg 4 Åpne data i offentlig sektor for mer informasjon.

**Sikkerhetsklassifisering**
Grad av beskyttelse som kreves for informasjonsobjektet. Hvis informasjonen, for eksempel mottatt post, kan ha flere klassifiseringsnivå, skrives «**Variabel**» i feltet.

Klassifiseringsnivå:

- **Åpen** informasjon kan være tilgjengelig for både eksterne og medarbeidere i virksomheten uten særskilte tilgangsrettigheter.

- **Intern** informasjon kan være tilgjengelig for både eksterne og medarbeidere i virksomheten med kontrollerte tilgangsrettigheter.

- **Konfidensiell** informasjon kan normalt kun være tilgjengelig for medarbeidere med strengt kontrollerte rettigheter. I spesielle tilfeller kan konfidensiell eller sensitiv informasjon også gjøres tilgjengelig for eksterne under samme strengt kontrollerte tilgangsrettigheter, for eksempel personopplysninger som etter avtaler skal kunne formidles til andre.

Noen virksomheter har informasjon som skal beskyttes etter beskyttelsesinstruksen og i sjeldne tilfeller etter sikkerhetsloven. Se vedlegg 5 Standarder, lover og forskrifter for mer informasjon.

**Sikkerhetsbehov**
Man tar her hensyn til spesielle sikkerhetsbehov ut fra informasjonsobjektenes konfidensialitet, integritet og/eller tilgjengelighet.

- **K** – Informasjonsobjektet inneholder sensitive opplysninger og skal behandles med **konfidensialitet**
- **I** – Informasjonsobjektets **integritet** skal beskyttes spesielt med hensyn til utilsiktede eller bevisste uautoriserte endringer
- **T** – Informasjonsobjektet skal behandles spesielt med hensyn til høy **tilgjengelighet**

**Maksimal nedetid**
Hvor lenge man kan akseptere at **elektronisk lagret** informasjonen er utilgjengelig. Akseptabel nedetid kan for noen systemer variere gjennom året i forhold til for eksempel eksamen, opptak, rapporteringer m.m. Anbefalte perioder er:

- **I TIME**
- **I DAG**
- **I UKE**
- **I MÅNED**

**Bevaringsverdi**
Bevaringsverdi er en vurdering som angir den relative betydningen informasjonen har for organisasjonen.

- **JUR** - Juridisk verdi
- **VIRK** – Virksomhetskritisk
- **HIST** - Historisk verdi

**Personopplysninger**
Hvis informasjonsobjektet inneholder eller kan inneholde personopplysninger, skal dette avmerkes i tabellen.

- **PERSONOPPLYSNINGER (P)** er opplysninger og vurderinger som kan knyttes til en enkeltperson.

- **SENSITIVE PERSONOPPLYSNINGER (S)** kan være opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.

**Arkivnøkkel**
En arkivnøkkel er et system for ordning av sakarkiv basert på ett eller flere ordningsprinsipper. Arkivnøkler beskriver inndelingsprinsipper og rekkeordningssystemer og benytter vanligvis et ordningsprinsipp på inndeling etter emne. Statlige organer skal i følge arkivforskriften bruke «Felles arkivnøkkel for statsforvaltningen». Det er laget en felles arkivnøkkel for statlige høgskoler. Den inneholder også en kassasjonsplan.

Ordning av emnegruppene, og dermed av mappene i det fysiske arkivet, gjøres etter desimalsystemet. Prinsippet i desimalsystemet er at emneområdene inndeles i inntil 10 grupper som nummereres med sifrene 0 - 9. Hver av disse gruppene blir igjen inndelt i 10 nye grupper, alle avledet av og bundet av det overordnede emnet. Disse kan igjen inndeles i 10'er-grupper, osv. Øverste nivå i hierarkiet kalles klasse.

Eksempel:
Klasse 1 er Økonomi
Hovedgruppe 13 er Regnskap og revisjon
Gruppe 133 er Avsluttet regnskap

**Oppbevaringsperiode**
Den tid som informasjonen skal oppbevares i arkivet. Oppbevaringsperioden starter når informasjonsobjekt blir til, og oppgis i antall år.

- **PERMANENT (PERM)** – informasjonsobjektet oppbevares permanent.
- **LEVETIDSRELATERT (LT)** – informasjonsobjektet er levetidsrelatert i forhold til andre objekter (datasystemer, prosjekter, programmer, kontrakter, bygninger, ansettelsesforhold, studieforhold eller lignende). Det er vanlig at man setter en oppbevaringsperiode som kan være 5 eller 10 år etter at objektet er avhendet, kontrakten er utløpt osv.
- **nn ÅR** – virksomheten har definert oppbevaringsperioden, for eksempel hvis oppbevaringsperiode er koblet til en hendelse, aktivitet eller er lovpålagt.

**Avhendingsregler**
Regler for avhending av informasjonen etter endt oppbevaringsperiode. Merk at det kan være spesielle regler for bevaring av informasjon som gjelder egen virksomhet eller som har prinsipiell karakter. Rutinemessige enkeltsaker som har mistet sin administrative betydning kan ofte kasseres.

- **GJENNOMGANG (GJG)** – send informasjonsobjektet til informasjonseieren for gjennomgang etter utløpt oppbevaringsperiode.
- **KASSER** – kasser informasjonsobjektet umiddelbart etter utløpt oppbevaringsperiode. Vær oppmerksom på at informasjonsobjekter som inneholder personopplysninger krever sikker destruering.
- **DEPONER** – deponer informasjonsobjekt i arkivdepot, for eksempel hos Statsarkivet, etter utløpt oppbevaringsperiode.
- **BEVARES** – skal ikke avhendes på grunn av krav om permanent oppbevaring.

## Vedlegg 1 Forslag til informasjonsklassifisering

Her er et forslag til informasjonsklassifisering for enkelte informasjonsobjekter som benyttes i universitets- og høgskolesektoren. Klassifiseringen informasjonsobjektene er basert på en kartlegging i sektoren, men inneholder ikke alle typer som benyttes i sektoren. Tabellen er ment som et utgangspunkt, og må gjennomgås og oppdateres av den enkelte virksomhet. Dette er spesielt viktig når det gjelder lagringssted, oppbevaringsperiode og avhendingsregler. Maksimal nedetid og arkivnøkkel kan også legges inn i tabellen. Kassasjonsplaner bør lages med utgangspunkt i virksomhetens arkivnøkkel.

| Eier | Innhold | Hjemmel | Lagrings-sted | Åpne data? (J/N) | Sikkerhets-klassifisering | Sikkerhets-behov | Maks. nedetid | Bevarings-verdi | Person-oppl.? | Arkiv-nøkkel | Oppbev.-periode | Avhending |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FOU | Forskningsprosjekter | offl. §26.4 | Artemis 7 Notur NorStore ePhorte Cristin | J/N | Intern | (K)IT | | VIRK, HIST | (PS) | | LT | GJG |
| FOU | FoU-søknader | offl. §26.4 | ePhorte | N | Intern | KIT | | - | - | | LT | GJG |
| FOU | FoU-tildelinger | | ePhorte | J | Åpen | I | | VIRK | - | | LT | GJG |
| FOU | Kontrakter | | ePhorte | J/N | Intern | KIT | | VIRK, JUR | (P) | | LT | GJG |
| PERS | Administrasjon av HMS | | | J/N | Åpen | I | | - | - | | LT | KASSER |
| PERS | Arbeidsavtaler | offl. § 13, §25.1, fvl. § 13.1 | ePhorte | N | Intern | KI | | JUR | S | | LT | KASSER |
| PERS | Arbeidsmiljøtiltak (én) | offl. § 13, fvl. § 13.1 | ePhorte | N | Intern | KI | | - | S | | LT | KASSER |
| PERS | Arbeidsmiljøtiltak (gruppe) | offl. § 13, §23.1, fvl. § 13.1 | ePhorte | N | Intern | (K)I | | - | S | | LT | KASSER |
| PERS | Disiplinærsaker | offl. § 13, fvl. § 13.1 | ePhorte | N | Konfidensiell | KI | | JUR | S | | LT | KASSER |
| PERS | Fagforeninger – drøfting | offl. § 14. §23.1 | ePhorte | N | Intern | (K)IT | | - | P | | LT | KASSER |
| PERS | Fagforeninger – drøfting - protokoll | | ePhorte | J/N | Åpen | I | | JUR | P | | LT | GJG |
| PERS | Likestillingsarbeid | | ePhorte | J/N | Åpen | I | | - | - | | LT | KASSER |
| PERS | Lønns- og personaldata | offl. § 13.1 jfr fvl. §13 | SAP HR | N | Intern | KIT | | VIRK, JUR | P(S) | | LT | KASSER |
| PERS | Lønnsforhandlinger | offl. §23.1 | ePhorte | J/N | Intern | KI | | VIRK, JUR | P | | LT | KASSER |
| PERS | Lønnsforhandlinger (én) | | | N | Intern | KI | | JUR | P(S) | | LT | KASSER |
| PERS | Medarbeidersamtaler | offl. § 13, fvl. § 13.1 Ikke i arkivet | | N | Konfidensiell | KI | | JUR | P(S) | | LT | KASSER |
| PERS | Omorganiseringer – prosess | offl. § 14, §23.1, fvl. § 18a | ePhorte | N | Intern | KI | | - | P(S) | | LT | GJG |
| PERS | Omorganiseringer - resultat | | ePhorte | J | Åpen | I | | VIRK | P | | LT | GJG |
| PERS | Oppfølging av sykdom | offl. § 13, fvl. § 13.1 | | N | Intern | KI(T) | | - | S | | LT | KASSER |
| PERS | Opprykk | offl. §23.1, § 25.1 | | N | Intern | (K)IT | | - | P | | LT | KASSER |
| PERS | Permisjoner | offl. § 13, fvl. § 13.1 | | N | Intern | KI | | - | P(S) | | LT | KASSER |
| PERS | Protokoller fra forhandlinger | | ePhorte | J/N | Åpen | I | | JUR, VIRK, HIST | P | | LT | GJG |

| Eier | Innhold | Hjemmel | Lagrings-sted | Åpne data? (J/N) | Sikkerhets-klassifisering | Sikkerhets-behov | Maks. nedetid | Bevarings-verdi | Person-oppl.? | Arkiv-nøkkel | Oppbev.-periode | Avhending |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PERS | Stipend | | | N | Intern | I | | - | P | | LT | KASSER |
| PERS | Taushetserklæringer | | ePhorte | N | Åpen | I | | JUR | P | | LT | KASSER |
| PERS | Tilsetting | offl. § 25 | | J/N | Åpen | I(T) | | - | P | | LT | KASSER |
| PERS | Tilsettingsinnstillinger | offl. § 25, fvl. § 13.1 | ePhorte | N | Intern | KI | | - | P | | LT | KASSER |
| PERS | Tilsettingssøknader | offl. § 25, fvl. § 13.1 | ePhorte | N | Intern | - | | - | P | | LT | KASSER |
| PERS | Varslingssaker | offl. § 13, fvl. § 13.1 | | N | Konfidensiell | KI | | JUR | S | | LT | KASSER |
| STUDA DM | Avviksmeldinger | | FS | N | Konfidensiell | KI | | JUR | P(S) | | LT | KASSER |
| STUDA DM | Avviksmeldinger studieprogresjon | offl. § 13.1 jfr fvl. §13 | FS | N | Intern | KIT | | JUR | P(S) | | LT | KASSER |
| STUDA DM | Eksamensoppgaver | Før eksamen: offl. § 26.1 | FS | N | Konfidensiell Åpen etter eksamen er gjennomført | KIT | | VIRK, HIST | | | PERM. | BEVARES |
| STUDA DM | Endring av personnummer | | FS | N | Intern | KI | | - | P | | LT | KASSER |
| STUDA DM | Fagplaner | | FS | J | Åpen | IT | | VIRK, HIST | - | | PERM. | BEVARES |
| STUDA DM | Fritak søknader | offl. § 13, fvl. § 13.1 | FS | N | Intern | KI | | - | P(S) | | LT | KASSER |
| STUDA DM | Fuskesaker | offl. § 13, fvl. § 13.1 | Plagiat-kontroll FS | N | Konfidensiell | KI | | JUR | S | | LT | KASSER |
| STUDA DM | Hospitant og privatistsøkn. | | FS | N | Intern | KI | | - | P(S) | | LT | KASSER |
| STUDA DM | Innplassering av fag | offl. § 13, fvl. § 13. | FS | N | Intern | KI | | - | P(S) | | LT | KASSER |
| STUDA DM | Internasjonalisering | offl. § 13 1. jfr fvl. §13 | FS | N | Intern | (K)IT | | - | P(S) | | LT | KASSER |
| STUDA DM | Klagesaker | offl. § 13, fvl. § 13.1 | Plagiat-kontroll FS | N | Intern | KI | | JUR | P(S) | | LT | KASSER |
| STUDA DM | Lånesaker (utenlandske stud) | offl. § 13 1.ledd jfr fvl. §13 | FS | N | Intern | (K)IT | | - | P(S) | | LT | KASSER |
| STUDA DM | Master- og PhD-avhandlinger | | FS | J/N | Åpen | IT | | HIST | | | PERM. | BEVARES |
| STUDA DM | Opptak | offl. § 13 .1 jfr fvl. §13 | FS | N | Intern | (K)IT | | VIRK | P(S) | | LT | KASSER |
| STUDA DM | Overflytting og linjeskift | offl. § 13, fvl. § 13.1 | FS | N | Intern | KI | | - | P(S) | | LT | KASSER |
| STUDA DM | Permisjoner | offl. § 13, fvl. § 13.1 | FS | N | Intern | KI | | - | P(S) | | LT | KASSER |
| STUDA DM | Sensorlister | | FS | J/N | Åpen | IT | | JUR | | | PERM. | BEVARES |
| STUDA DM | Sensur og eksamensbehandling | offl. § 26.3 | Plagiat-kontroll FS | N | Konfidensiell | KIT | | JUR | P | | LT | KASSER |
| STUDA DM | Skikkethetssaker | offl. § 13, fvl. § 13.1 | FS | N | Konfidensiell | KI | | JUR | S | | LT | KASSER |
| STUDA DM | Studieplaner (institusjon) | | FS | J | Åpen | IT | | VIRK, HIST | - | | PERM. | BEVARES |
| STUDA DM | Studieveiledning | offl. § 13, fvl. § 13. | FS | N | Intern | KI | | - | P(S) | | LT | KASSER |

| Eier | Innhold | Hjemmel | Lagrings-sted | Åpne data? (J/N) | Sikkerhets-klassifisering | Sikkerhets-behov | Maks. nedetid | Bevarings-verdi | Person-oppl.? | Arkiv-nøkkel | Oppbev.-periode | Avhending |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| STUDA DM | Tilrettelegging | offl. § 13, fvl. § 13.1 | FS | N | Intern | KI | | - | S | | LT | KASSER |
| STUDA DM | Vitnemål | § 26.3 | FS | N | Intern | (K)IT | | HIST | P | | PERM. | BEVARES |
| STYRER, RÅD og UTVALG | Innkallinger | offl. § 13, fvl. § 13. | ePhorte | J/N | Intern | KIT | | - | P | | LT | KASSER |
| STYRER, RÅD og UTVALG | Protokoller | offl. § 13, fvl. § 13. | ePhorte | J/N | Intern | (K)IT | | VIRK, HIST, JUR | P(S) | | PERM. | BEVARES |
| ØKO | Anbud og innkjøp | offl. §23.3, §13.1 jf forvalt. L 13.1 andreledd | KGV Basware.Invoice Basware PM Agresso ePhorte | J/N | Intern | KIT | | VIRK, JUR | - | | LT | GJG |
| ØKO | Avtaler og kontrakter | offl. §23.1 | ePhorte | J/N | Intern | KIT | | VIRK, JUR, HIST | - | | LT | GJG |
| ØKO | Budsjett og bevilgning | offl. §23.1, §23.1 | ePhorte | J/N | Intern | KIT | | VIRK | - | | LT | GJG |
| ØKO | Internkontroll | | | J/N | Variabel | KIT | | VIRK | - | | LT | GJG |
| ØKO | Prosjekter | | Artemis 7 | J/N | Variabel | KIT | | VIRK | - | | LT | GJG |
| ØKO | Rapport og planer | | ePhorte | J | Åpen | I | | VIRK, HIST | - | | LT | GJG |
| ØKO | Regnskapsrapporter | | Agresso | J | Åpen | I | | JUR, HIST | - | | 10 år | KASSER |
| ØKO | Tildelinger av midler | | ePhorte | J | Åpen | I | | VIRK | - | | LT | KASSER |
| ØKO | Økonomiregelverk | | ePhorte | J | Åpen | I | | - | - | | LT | KASSER |
| ØKO | Årsmeldinger | | ePhorte | J | Åpen | I | | HIST | - | | PERM. | BEVARES |

## Vedlegg 2 Om arkivering

Skillet mellom arkiv, bibliotek og samling (dokumentsamling) kan kort forklares ved at et **arkiv** består av brev eller dokumenter som er blitt til som ledd i en bedrifts eller et (offentlig) organs virksomhet. Arkivdokumentene er ofte samlet innenfor en sak og er i liten grad mangfoldiggjort (består ofte av unike dokumenter, men rundskriv og andre mangfoldiggjorte dokumenter kan også inngå i et arkiv).

Et **bibliotek** består av en samling av mangfoldiggjorte dokumenter (bøker, tidsskrifter).

En **samling** kan ofte bestå av unike dokumenter, men disse er da samlet ut fra et annet perspektiv enn å dokumentere en prosess eller en saksbehandling. Eksempelvis vil en samling av brev fra en (kjent) person over mange år normalt ikke kalles et arkiv dersom de er samlet inn i ettertid.

Både privatpersoner, bedrifter og offentlige organer har arkiver i varierende grad. Offentlige organer er pålagt å ha arkiv etter bestemte regler for å dokumentere sin virksomhet.

**Noark**
Noark er en forkortelse for **Norsk arkivstandard**. Noark ble utarbeidet som en kravspesifikasjon for elektroniske journalsystemer i statsforvaltningen i 1984 av Statens rasjonaliseringsdirektorat (Statskonsult) i samarbeid med Riksarkivaren, og den etablerte seg raskt som de facto standard.

Noark 5 er gjeldende standard i dag. Videreutviklingen har omfattet dels modernisering i tråd med den teknologiske utviklingen, dels utvidelser i systemenes informasjonsinnhold og funksjonalitet.

Noark er både en felles standard for offentlig forvaltning og et hjelpemiddel for å øke samhandlingen mellom systemer og organer. Et avleveringsuttrekk laget etter Noark5 er egnet til langtidslagring. Private virksomheter vil også ha nytte av Noark.

Arkivforskriften § 2-9 sier at offentlige organer normalt skal benytte et Noark-godkjent system ved elektronisk journalføring og arkivering.

Eksempel på Noark-godkjente systemer:

- ePhorte fra EVRY og Gecko
- Documentum fra Ciber og Joint
- Visma samhandling arkiv

## Vedlegg 3 Bevarings- og kassasjonsplan

Hovedformålet med å gjennomføre arkivbegrensning (1) og kassasjon er både å redusere omfanget av papirarkivene, men også å strukturere og tilrettelegge informasjon i elektroniske arkiver. Samtidig skal det sikres at arkivmateriale som har varig verdi blir bevart for ettertiden.

Det er først og fremst økonomiske hensyn som gjør at det oppstår behov for kassasjon. Andre hensyn gjør det nødvendig med påbud om tidsbegrenset bevaring av arkivsaker:

- Enkeltpersoners behov og juridiske rettigheter må kunne dokumenteres
- Virksomhetens eget behov for presedens og likebehandling i saksbehandlingen, og som dokumentasjon på eiendomsrett, økonomiske og juridiske rettigheter
- Forskningen må sikres et tilstrekkelig og representativt kildemateriale

**Utarbeiding av forslag til bevarings- og kassasjonsregler**
Arkivforskriften § 3-21 pålegger statlige organer å utarbeide forslag til kassasjonsregler for eget organ. Dette innebærer at organet skal lage en oversikt over hva slags arkivmateriale som skal bevares for ettertiden og hva slags materiale som skal kasseres. En slik oversikt kalles ofte en bevarings- og kassasjonsplan (bk-plan), fordi den også inneholder frister for kassasjon som skal følges opp.

**Bevarings- og kassasjonsplan eller enkel kassasjonssøknad?**
Dersom et organ ønsker å kassere en enkelt serie eller bevarings- og kassasjonsvurdere et enkelt system, er det tilstrekkelig å sende inn en kassasjonssøknad. Ta derfor kontakt med Riksarkivet for å få råd om hva som er mest hensiktsmessig i det aktuelle tilfellet.

**Hva skal bevarings- og kassasjonsplanen inneholde?**
Bevarings- og kassasjonsplanen skal inneholde følgende:

- En kartlegging, det vil si en systematisk og grundig undersøkelse og beskrivelse, av forvaltningsorganets, etatens eller sektorens ansvarsområder, funksjoner og arkiver.
- En bevarings- og kassasjonsvurdering, dvs. en vurdering av hvilke arkiver som skal bevares for ettertiden og hvilke som skal kasseres, samt en begrunnelse for hvorfor arkivene skal bevares eller kasseres
- Kassasjonsfrister

Se også Arkivverkets hjemmesider http://www.arkivverket.no/

(1) Med arkivbegrensning menes at det ikke registreres eller arkiveres materiale som er uten verdi for senere saksbehandling eller dokumentasjon.

## Vedlegg 4 Åpne data i offentlig sektor

Både Fornyings-, og administrasjons- og kirkedepartementet (FAD) og Direktoratet for forvaltning og IKT (Difi) ønsker å legge forholdene til rette for at offentlige virksomheter skal dele sine data slik at de kan brukes i nye sammenhenger og til nye tjenester. Tilgjengeliggjøring og viderebruk av offentlige data handler om å la næringsliv, forskere og sivilsamfunn få tilgang til og gjøre nytte av informasjon forvaltningen har.

Med begrepet offentlige data menes alle typer informasjon som er produsert eller samlet inn av offentlige virksomheter. Offentlige data er i all hovedsak informasjon som er eller kan bli digitalisert og lagret elektronisk. Offentlige data kan for eksempel være næringslivsregistre, kartdata, organisasjonsmodeller, budsjett, årsregnskap og lignende. Når data blir gjort tilgjengelige i et maskinlesbart format, blir det mulig for andre å finne nye måter å bruke dataene på. På denne måten kan nytteverdien av data produsert av det offentlige mangedobles. I tillegg gir det en åpnere og mer legitim forvaltning og økt samhandling i offentlig sektor.

Å tilgjengeliggjøre data for viderebruk handler i mange tilfeller om mer enn å publisere informasjon slik at det er mulig å bla i data på en nettside. Viderebruk handler også om at rådata gjøres tilgjengelig i det som kalles «maskinlesbare formater», slik at datamaskiner kan brukes til å tolke og analysere datamaterialet. Rådata er data som kan prosesseres maskinelt, tas fra hverandre, blandes med andre data og brukes i nye sammenhenger.

### Veileder fra Difi

Veilederen gir en innføring i hvordan offentlige data kan gjøres tilgjengelig for videre bruk, og inneholder blant annet:

- Eksempler på hva åpne data kan brukes til
- Argumenter for hvorfor offentlige virksomheter bør dele sine data
- Praktiske råd til hvordan det kan gjøres

http://data.norge.no/blogg/2012/05/veileder-i-tilgjengeliggj%C3%B8ring-av-offentlige-data

### Retningslinjer ved tilgjengeliggjøring av offentlige data fra FAD

For å sikre at data blir tilgjengeliggjort på en hensiktsmessig måte bør offentlige virksomheter tilgjengeliggjøre data i tråd med FADs retningslinjer som omhandler:

- Gratisprinsippet
- Maskinlesbare formater
- Bearbeiding
- Dokumentasjon
- Opphavsrett
- Synliggjøring
- Tilbakemeldinger
- Fast adresse

Retningslinjene er beskrevet her: http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2012/retningslinjer-ved-tilgjengeliggjoring-a.html?id=708912

**Digitaliseringsrundskrivet P-10/2012**
Rundskrivet gir føringer for hvordan virksomhetene skal digitalisere for å tilby bedre tjenester og effektivisere driften. Det inneholder viktige pålegg og anbefalinger fra ulike regelverk og beslutninger sentralt, for å lette oversikten for virksomhetene. I tillegg redegjør rundskrivet for prosessen med IKT-relaterte investeringer i 2014-budsjettet.

http://www.regjeringen.no/nb/dep/fad/dok/rundskriv/2012/digitaliseringsrundskrivet.html?id=706462

**NLOD - Norsk lisens for åpne data**
Fornyings-, administrasjons- og kirkedepartementet har utarbeidet en lisensavtale som offentlige virksomheter kan bruke ved tilgjengeliggjøring av data. Når data er lisensiert med norsk lisens for offentlige data (NLOD) kan de fritt viderebrukes på visse vilkår.

Lisensen gir lov til
- å kopiere og tilgjengeliggjøre
- å endre og/eller sette sammen med andre datasett
- å kopiere og tilgjengeliggjøre en endret eller sammensatt versjon
- å benytte datasettet kommersielt

På følgende vilkår
- at man navngir lisensgiver slik lisensgiver ber om, men ikke på en måte som indikerer at disse har godkjent eller anbefaler deg eller din bruk av datasettet
- at man ikke bruker dataene på en måte som fremstår som villedende, og heller ikke fordreier eller uriktig fremstiller dataene

Med den forståelse
- at data som inneholder personopplysninger og er taushetsbelagt, ikke er omfattet av denne lisensen og ikke kan viderebrukes
- at lisensgiver fraskriver seg ethvert ansvar for informasjonens kvalitet og hva informasjonen brukes til

Norsk lisens for offentlige data (NLOD) er tilgjengelig både på norsk og på engelsk.

http://data.norge.no/nlod/en

**Datahotellet data.norge.no**
Data.norge.no er et register over åpne data i Norge. Her tilbys også et datahotell for virksomheter som ønsker å bruke Difis tekniske infrastruktur til å publisere egne data i maskinlesbare formater.

http://data.norge.no

## Vedlegg 5 Standarder, lover og forskrifter

**Noark 5 - Norsk arkivstandard**
http://www.arkivverket.no/arkivverket/Offentlig-forvaltning/Noark/Noark-5/Standarden

Beskrives i vedlegg 1 Om arkivering.

**Arkiv og kassasjonsplan for de statlige høgskolene**
www.khio.no/intranett/filestore/arkivnokkel_**kassasjonsplan**.doc
Planen ligger tilgjengelig på hjemmesidene hos flere institusjoner, men her er for enkelhets skyld valgt en lokasjon.

Arkivplanen er opprinnelig fra 1994. Kassasjonsplanen ble lagt til i mai 2001. Sist revidert i juni 2005. En ny versjon av planene vil bli utarbeidet i 2013.

**Arkivloven**
LOV 1992-12-04 nr 126: Lov om arkiv
http://www.lovdata.no/all/nl-19921204-126.html

**Arkivforskriften**
FOR 1999-12-01 nr 1566: Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver
http://www.lovdata.no/for/sf/ku/xu-19991201-1566.html.

Forvaltningens arkivfunksjon har i lang tid vært regulert gjennom et eget regelverk. Forskriften kom som et resultat av behovet for ytterligere regulering blant annet for å regulere elektronisk arkivering av arkivmateriale. Sammen utgjør arkivloven og arkivforskriften kjernen i det regelverket som regulerer håndtering av offentlige arkiver.

Arkivloven gir en del overordnede og grunnleggende bestemmelser om arkiv og spesielt om arkiv i offentlig forvaltning. Bestemmelsene gjelder, med få unntak jf. arkivloven § 5, for all virksomhet som utøves av den offentlige forvaltning.

Formålet med arkivloven er å sikre arkiv som har betydelig kulturell eller forskningsmessig verdi, eller som inneholder rettslige eller viktig forvaltningsmessig informasjon, slik at disse kan bli tatt vare på og gjort tilgjengelige for ettertiden, jf. arkivloven § 1. Videre fastsetter arkivloven i § 6 at offentlige organ plikter å ha arkiv, og at disse skal ordnes og innrettes slik at dokumentene er sikret som informasjonskilder for samtid og ettertid.

Sammen med de utfyllende forskriftene representerer loven et helhetlig juridisk rammeverk rundt alle arkivrelaterte spørsmål i offentlig forvaltning, helt fra dokumentet oppstår som ledd i den daglige virksomheten, via arkivbegrensning og avlevering av bevaringsverdig arkiv-materiale til arkivdepot, og under oppbevaring og tilgjengeliggjøring for ettertiden.

**Forvaltningsloven**
LOV 1967-02-10 nr 00: Lov om behandlingsmåten i forvaltningssaker
http://www.lovdata.no/all/hl-19670210-000.html

Loven regulerer visse typer arkivmateriale gjennom bestemmelser om hvilke regler som gjelder for saksbehandling, og om hvilke rettigheter forvaltningsloven gir den enkelte. Formålet med loven er å regulere de rettigheter borgerne har når de er i kontakt med offentlige instanser. Forvaltningsloven skal ivareta rettssikkerheten til borgerne og sikre en betryggende saksbehandling. Loven er en overordnet lov som tas i bruk i all saksbehandling, så lenge ikke annen lov gjelder etter særlovgivning.

**Offentleglova**
LOV 2006-05-19 nr 16: Lov om rett til innsyn i dokument i offentleg verksemd
http://www.lovdata.no/all/hl-20060519-016.html

Formålet med lova er å leggje til rette for at offentleg verksemd er open og gjennomsiktig, for slik å styrkje informasjons- og ytringsfridommen, den demokratiske deltakinga, rettstryggleiken for den enkelte, tilliten til det offentlege og kontrollen frå ålmenta. Lova skal òg leggje til rette for vidarebruk av offentleg informasjon.

**Pliktavleveringslova**
LOV-1989-06-09-32: Lov om avleveringsplikt for allment tilgjengelege dokument
http://www.lovdata.no/all/hl-19890609-032.html

Føremålet med denne lova er å tryggja avleveringa av dokument med allment tilgjengeleg informasjon til nasjonale samlingar, slik at desse vitnemåla om norsk kultur og samfunnsliv kan verta bevarte og gjorde tilgjengelege som kjeldemateriale for forsking og dokumentasjon.

**Personopplysningsloven**
LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger
http://www.lovdata.no/all/hl-20000414-031.html

Loven omfatter behandling av personopplysninger med elektroniske hjelpemidler, og manuell behandling av personopplysninger som innebærer opprettelse av et personregister.

Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

**eForvaltningsforskriften**
FOR-2004-06-25-988 Forskrift om elektronisk kommunikasjon med og i forvaltningen
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html

Formålet med forskriften har vært å utarbeide et felles regelverk som legger rammene for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Forskriften skal fremme forutsigbarhet og fleksibilitet, samt legge til rette for samordning av sikre og hensikts-

messige tekniske løsninger, herunder e-signatur.

eForvaltningsforskriften inneholder bestemmelser som gir føringer for rutiner og prosedyrer knyttet til arkivdanningen.

**Sikkerhetsloven**
LOV-1998-03-20-10 Lov om forebyggende sikkerhetstjeneste
http://www.lovdata.no/all/hl-19980320-010.html

Lov om forebyggende sikkerhetstjeneste har et eget kapittel om informasjonssikkerhet.

Formålet med loven er ved forebyggende tiltak å trygge rikets sikkerhet og vitale nasjonale sikkerhetsinteresser mot spionasje, sabotasje og terrorhandlinger, og gjelder for hele forvaltningen. Loven skal dessuten ivareta den enkeltes rettssikkerhet og trygge tilliten til og forenkle kontrollen med tjenesten. Tiltakene skal implementeres i stat, kommune og private virksomheter som loven gjelder for.

Det er utarbeidet forskrifter innen informasjonssikkerhet, personellsikkerhet, industrisikkerhet og sikkerhetsadministrasjon. For arkivmessig behandling av dokumenter gradert etter sikkerhetsloven, er det særlig forskrift om informasjonssikkerhet som er aktuell.

Informasjon som skal beskyttes etter **Sikkerhetsloven** har følgende sikkerhetsgrader:

- **BEGRENSET** nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- **KONFIDENSIELT** nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- **HEMMELIG** nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- **STRENGT HEMMELIG** nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

**Forskrift om informasjonssikkerhet**
FOR-2001-07-01-744: Forskrift om informasjonssikkerhet
http://www.lovdata.no/for/sf/fo/xo-20010701-0744.html

Forskriften har samme formål og virkeområde som sikkerhetsloven.

**Beskyttelsesinstruksen**
FOR 1972-03-17 nr 3352: Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter
http://www.lovdata.no/for/sf/in/xm-19720317-3352.html

Instruks av for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen), omfatter dokumenter uavhengig av mediet de er tilgjengelig på.

Beskyttelse av et dokument etter beskyttelsesinstruksen skal bare foretas når dokumentet kan unntas fra offentlighet i medhold av offentleglova og skadevirkninger kan inntreffe.

Informasjons som skal beskyttes etter **Beskyttelsesinstruksen** har følgende beskyttelsesgrader:

- **FORTROLIG** benyttes dersom det vil kunne skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.
- **STRENGT FORTROLIG** benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.

**Stortingsmelding nr. 8 (2012 – 2013) Eksport av forsvarsmateriell fra Norge i 2011, eksportkontroll og internasjonalt ikke-spredningssamarbeid**

http://www.regjeringen.no/nb/dep/ud/dok/regpubl/stmeld/2012-2013/meld-st-8-2012--2013.html?id=707794

Regjeringens melding til Stortinget om omfanget av eksporten av forsvarsmateriell. I tillegg redegjøres det for norsk eksportkontrollpolitikk, regelverket og det internasjonale arbeidet når det gjelder eksportkontroll og ikke-spredning. Kapittel 3.3 tar for seg kontroll med kunnskapsoverføring til utenlandske studenter ved norske læresteder.

Ved spørsmål omkring denne eller andre UFSer – kontakt campus@uninett.no
Andre UFSer er tilgjengelige på www.uninett.no/ufs