# MUSIT universitetsmuseenes IT-organisasjon
# Handlingsplan for innføring av GDPR i MUSIT 2018 -2019

## *Bakgrunn og målsetning*

Den Europeiske Unions (EU) forordning for personvern, The General Data Protection Regulation (GDPR), trådte i kraft i EU 25. mai 2018, og i Norge 20. juli 2018 (Lov om behandling av personopplysninger). Med dette vil kravene for å behandle personopplysninger innskjerpes ytterligere.

Universitetsmuseenes IT-organisasjon MUSIT er involvert i behandling av personopplysninger knyttet til de seks universitetsmuseene; Arkeologisk museum, NTNU Vitenskapsmuseet, Universitetsmuseet i Bergen, Kulturhistorisk museum, Naturhistorisk museum, og Tromsø museum. Våren 2018 gjennomført Eirik Rindal (UiO/Naturhistorisk museum), Bjørn Petter Løvfall (UiO/Naturhistorisk museum) og Susan Matland (MUSIT) et innføringskurs i GDPR ved BI i Oslo med MUSIT som case. Hovedmålet med kurset var å gjennomføre en evaluering av MUSITs virksomhet i forhold til GDPR og de områder MUSIT lager personopplysninger. Dette arbeidet danner grunnlag for handlingsplanen for innføring av GDPR i MUSIT.

| | |
|---|---|
| **Hovedmål** | Å sikkert at personopplysninger som lagres i MUSIT-basene gjøres i henhold til nye personvernloven (GDPR). |
| **Effektmål** | En enhetlige behandling av personopplysninger i MUSIT.<br><br>Økt kvalitet på data som genereres og lagres. |
| **Resultatmål / Gevinster** | Felles rutiner for innføring av personopplysninger i MUSIT-basene.<br><br>Økt oppmerksomhet og bevissthet om personvern ved museene og i tilknytning til bruk av data.<br><br>Museene vil bli mer oppmerksomme på hvilke typer personopplysninger som lagers og eventuelt brukes. |

# Vurdering av personopplysninger som lagres i regi av MUSIT sett opp mot GDPR [1]

## *Universitetsmuseenes innsamling og lagring av personopplysninger*

Det er særlig i følgende tilfeller at museene samler inn navn og opplysninger om personer som eventuelt må tilpasses GDPR krav om vern av fysiske personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger, samt om oppheving av direktiv.

I forbindelse med innsamling av museumsobjekter lagres navnene på innsamlerne i MUSIT-baser. I tilknytning til objektene lagres også hvor og når de er samlet inn, slik at man indirekte kan se hvor en person har vært på et gitt tidspunkt eventuelt hvem vedkommende har vært sammen med når flere personer står bak innsamlingen.

1. Som en del av kvalitetssikringen av arbeidet med navn på innsamlere, lagres informasjon om når en person er født og eventuelt døde, og også om en person har skiftet navn i løpet av sin levetid. På denne måte er det mulig å holde flere samlere med samme navn fra hverandre eller føre ulike samlenavn til samme person.

2. Brukere av museumsgjenstander kan være alt fra egne forskere og ansatte, gjesteforskere fra andre universiteter i verden, ikke-profesjonelle fageksperter og statsstipendiater, og allmennhet. Det er vanlig at objekter blir studert av andre og informasjon om objektet blir da ofte revidert. I forbindelse med dette blir navnet til den som har gjennomført en revisjon lagret i databasen.

3. Fotografier. I MUSIT-basene fins det betydelige mengder med fotografier. Navn på fotograf, tid og sted for fotograferingen, og navn på dem som er avbildet lagres i basen hvis det er kjent.

4. Det lagres opplysninger om hvem som har registrert opplysningene i databasene, og når dette ble utført, dvs. hvem som er saksbehandler og når saken er behandlet.

[1] Det har tidligere vært avklart med datatilsynet at lagringen av personopplysning er i tråd med gjeldene (pre-GDPR) regelverk (Svarbrev fra Datatilsynet – Jnr. 2009/18860-3).

**Følgende personopplysninger samles og lagres:**

Innsamlere og personer som reviderer materiale: navn og synonymer av navn, fødsel- og eventuelt dødsdato, tittel/yrkesbakgrunn som f.eks. Herr, Professor, Dr., Mrs., lenker til nettressurser/ ID-nøkkel, fødested, adresse, kommune, land, arbeidssted. Disse regnes ikke som personlige forhold etter forvaltningslovens § 13 og er dermed ikke innbefattet av taushetsplikten.

***Lagring***

Dataene lagres på to hovedmåter:

**A.** Informasjonen ligger fysisk sammen med objektet som en papiretikett, ofte med henvising til skriftlig materiale i arkiv.

**B.** Digitalisert informasjon lagres elektronisk på flere servere. Logging av saksbehandlernes arbeid i databasene lagres kun elektronisk. Det er kun museumsansatte og IKT-avdelingene ved universitetene som har full tilgang til disse dataene ved behov. Tilgangen er styrt etter behov og går via sikre innloggingstjenester (https://www.feide.no/ og https://www.uninett.no/tjenester/dataporten).

***Universitetsmuseenes samlinger har allmenn interesse***

I følge GDPR, samt ny personopplysningslov, gis det adgang til å behandle og lagre personopplysninger som har allmenn interesse og for vitenskapelige og historisk forskning (forordning (EU) 2016/679, GDPR generelle bestemmelser art. 50, art. 5 nr. 1 bokstav b og e, art. 9 nr. 2 bokstav e, art. 89, Proposisjon 56 LS (2017–2018) med forslag til ny personopplysningslov §§ 8 og 9). Article 29 data protection working party (heretter Working party 29) har uttalt at arkiver og museer kommer inn under det man kan oppfatte som i allmennhetens interesse (Working party 29 (2016) 207 s. 2).

***Universitetsmuseene deler data nasjonalt og internasjonalt***

Stortinget har uttalt at museene må dele sine data, også via internett (Stortingsmelding nr. 15 (2007-2008, Tingenes tale Universitetsmuseene, side 11), og at «det bærende prinsipp må være at museene har ansvar for å tilrettelegge og tilgjengeliggjøre egne data gjennom åpne grensesnitt basert på internasjonale standarder og utvekslingsformater» (Stortingsmelding nr. 15 (2007-2008), Tingenes tale Universitetsmuseene, side 33).

Unntak fra dette er som regel der det er sårbare lokaliteter eller objekter, eksempelvis helleristningsfelter, rovfuglreir, eller sjeldne orkideer. Regjeringen har via digitaliseringsrundskrivet gitt sterke føringer for at digitale løsninger skal utvikles gjennom hele statsapparatet. Og det anbefales at data skal tilrettelegges for gjenbruk og videre bruk i EØS-området (KMD (2017) «Retningslinjer ved tilgjengeliggjøring av offentlige data.» og Digitaliseringsrundskrivet av 08.09.2017).

Mussenes data med objektinformasjon, og personer som er knyttet til objektene, deles fritt ut på internett blant annet via, MUSITs egen nettportal UNIMUS (http://www.unimus.no), Global Biodiversity Information Facility (GBIF) (https://www.gbif.org), Artskart fra Artsdatabanken (https://artskart.artsdatabanken.no), Riksantikvarens Askeladden (https://www.riksantikvaren.no/Veiledning/Data-og-tjenester/Askeladden), Norvegiana (https://norvegianablog.wordpress.com/), og Europeana (https://www.europeana.eu/portal/no). Navn på samlerne blir tilgjengelig via søk etter andre tema/kriterier som f.eks. geografi eller objekttype.

Slik tilgjengeliggjøring har støtte fra Working party 29 «Against this background, one of the key policy objectives of the PSI (Public sector information) Amendment is to introduce the principle that all public information (that is, all information held by the public sector, which is publicly accessible under national law) is reusable for both commercial and non-commercial purposes» (Working party 29 (2016) 207 s. 2).

***Klargjøring av rollene behandlingsansvarlig og databehandler***

Det er mange aktører rundt delingen av dataene fra museenes samlinger. En klargjøring av hvem som har hvilke roller er avgjørende for godt personvern.

*Behandlingsansvarlig*

Behandlingsansvarlig er definert av GDPR (art.4 (7)) som den som bestemmer hvordan behandlingen av personopplysninger skal utføres. De behandlingsansvarlige i denne sammenhengen er hvert enkelt museum.

Museene er behandlingsansvarlig. Museene bestemmer hvordan man skal samle inn, og fylle ut data i databasene. Alle museene har skrevne eller uskrevne regler for hvordan data skal skrives inn og kvalitetssikres. Det er også museene som eier disse dataene.

Videre utleveres data til GBIF, Artsdatabanken, Norsk kulturråd (eier av Norvegiana) og Riksantikvaren (eier av Askeladden), som legger ut informasjon på internett. Disse betraktes også som behandlingsansvarlig. Working party 29 har uttalt (Working party 29 (2008) 148 s.14) at søkemotorer er underlagt EUs regelverk om personvern hvis de lager lokale kopier av innholdet, noe som er tilfellet med disse dataportalene.

*Databehandler*

Databehandler er definert i GDPR (art.4 (8)), som den som behandler personopplysninger på vegne av behandlingsansvarlig. Det er flere databehandlere, i tillegg til at museene selv behandler data, kjøper de også tjenester for å registrere museumsobjekter. Databehandlerne kan deles inn i:

**A.** Primær databehandler: UiO/USIT og;

**B.** Innskriversentraler: som Alembo, og Digforsk AS som museene kjøper tjenester av og hvor dataene slettets hos dem etter endt oppdrag.

UiO/USIT er databehandler da de i tillegg til å vedlikeholde databasene også, på ordre fra museene, foretar endringer i personopplysninger.

Innskriversentraler som DigForsk AS og Alembo (via Picturae, Nederland) som spesialiserer seg på å overføre analoge data til digitale format er også å betrakte som databehandlere. Alembo er av spesiell interesse da denne befinner seg i Surinam, Sør-Amerika, og berøres av regelverk for overføring til tredjepart/land (GDPR art 4 (10). Hvert museum må sørge for at EUs standard personvernbestemmelser (Standard Contractual Clauses) undertegnes ved bruk av slike innskriversentraler.

MUSIT er **ikke** å betrakte som behandlingsansvarlig eller databehandler da organisasjonen ikke faller inn under definisjonene for hverken behandlingsansvarlig eller databehandler (GDPR art. 4 nr. 8 og nr. 9).

***Behov for DPIA?***

Personvernskonsekvensvurdering (data protection impact assessment, heretter DPIA) er et viktig verktøy i GDPR, og skal gjennomføres hvis det er sannsynlig at behandlingen vil medføre høy risiko for fysiske personers rettigheter og friheter (GDPR art. 35 nr.1).

Kriteriene for når en DPIA er nødvendig er ved **1**. Systematiske og omfattende vurdering av personlige aspekter, **2**. Behandling i stor skala av særlige kategorier data, **3**. Systematisk overvåkning i stor skala av offentlige område. Vi anser det som unødvendig med en DPIA for MUSITs databaser, da omfanget av personopplysninger og antallet personer er av svært begrenset karakter (GDPR art. 35 nr. 3 bokstav a til c).

Behandling av personopplysninger i særlige kategorier (GDPR art. 9) det som tidligere ble kalt sensitive opplysninger, krever spesielle forhåndsregler og tiltak. Vi har vurdert at personopplysninger i MUSIT ikke faller inn under denne kategorien, med ett unntak: MUSITs samlings/forvaltningsarkiv -**TopArk** (Topografisk arkivet).

**TopArk** (Topografisk arkiv) applikasjon er brukt ved to av museene; Vitenskapsmuseet og Universitetsmuseet i Bergen. Her er det lagret opplysninger om lovovertredelser, for eksempel hærverk på kulturminner (GDPR art. 10). I tilknytning MUSIT er museenes hovedformål å ta vare på og skape kunnskap rundt kultur- og naturgjenstander. Kunnskap om at et kulturminne har vært utsatt for hærverk kan være av stor betydning for forvaltningen av objektet. Men kunnskap om hvem som har utført hærverket kan ikke sies å være en del av dette og slik informasjon og skal ikke lagres i MUSITs samlings/forvaltningsarkiv TopArk. Museene må gjøre en vurdering om hvordan slik opplysning skal håndteres og eventuelt lagres.

Totalt sett er personopplysningene som lagres ikke omfattende og antall personer som er laget relativt få. Det er også relativt få personer som behandler person-opplysningene. Begrunnelsen for behandlinger er vitenskapelig formål og allmennhetens interesse.

# Vurdering av MUSIT og museenes behandling av personopplysninger

## *Lovligheten*

*Formålet*

Formålet med innsamlingen og behandlingen av personopplysninger i forbindelse med museenes samlingsarbeid, anses å være lovlig etter GDPR art. 5 nr. 1 bokstav b som spesifikt gir hjemmel for «formål knyttet til vitenskapelig eller historisk forskning […] (GDPR art. 89 nr.1). Personopplysningen samles inn for å kunne identifisere innsamler, hvor og når, og eventuelt hensikten med innsamlingen. Formålet med innsamlingen av personopplysninger er å kunne knytte opplysninger om innsamlingshendelsen til objektet. Objekts vitenskapelige verdi er uløselig knyttet til konteksten det ble funnet i.

Det har vært diskutert om tilgang til opplysning om saksbehandler i databasene kun bør være tilgjengelig for administratorer. Men museene anser det som viktig å vite hvem som har gjort hva med samlingene, samt at alle saksbehandlere bør ha tilgang til denne informasjonen. Dette er kun for internt og forvaltningsmessig bruk.

Loggføring av hvem som utfører saksbehandling anses å falle inn under arbeids-miljøloven § 9-1, og er en del av arbeidsgivers styringsrett. Utover dette er begrunnelsen for å lagre personopplysninger knyttet til saksbehandlingen den samme som for å lagre data om innsamlere av gjenstandene (allmenn interesse og vitenskapelige formål) og vil i det neste bli behandlet likt.

*Behandlingen*

Behandlingen av personopplysninger anses å være lovlig (GDPR art. 6 nr.1 bokstav e) da «behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse». Det kreves at det skal være nasjonalt rettsgrunnlag for behandlingen (GDPR art. 6 nr. 3 bokstav b). Rettsgrunnlaget finnes i UHL § 1-4 (2), for kulturhistoriske gjenstander er denne oppgaven videre spesifisert i forskrift etter kulturminneloven (Forskrift nr. 8785 om faglig ansvarsfordeling mv. etter kulturminneloven, §1 og §2).

Gjenbruk (viderebehandling) av dataene til andre formål er unntak fra regelen om at personopplysninger kun skal brukes til det formålet de ble samlet inn for, da det er snakk om formål knyttet til vitenskapelig forskning (GDPR art 5. nr. 1 bokstav b).

*Omfanget*

Omfanget av personopplysningene som samles inn skal være begrenset til hva som anses som nødvendig (GDPR art 5. nr. 1 bokstav c). For museene begrenes dette til nødvendige opplysninger om innsamler. Det samles inn, navn tittel, fødselsdato (og eventuelt dødsdato) samt link/ID-nøkkel til andre åpne nettressurser om personen. Det er nødvendig å vite når personen er født (og død) slik at man sjekke kvaliteten av dataene. Link/ID nøkkel til andre nettressurser om personen er av betydning for å kunne koble datasett, heve kvaliteten på dataene, samt å spare det offentlige for utgifter ved å unngå dobbeltarbeid.

Avdøde innsamlere er ikke omfattet av GDPR (generelle bestemmelser nr. 27). Men det er uttalt at i museums-samlinger kan det være behov for skjerming av personopplysninger selv om de omfatter døde personer (Arbeidsgruppen 29 WP 207 (05.06.2013) avsnitt IX. s. 23). Vi vurderer det dithen at dette ikke kommer til anvendelse for personopplysninger i forbindelse med innsamling av objekter, da disse opplysningene er svært begrenset i sitt omfang.

*Perioden*

Personopplysningene skal ikke lagres lengre enn det som er nødvendig (GDPR art. 5 nr. 1 bokstav e). Museumssamlinger skal i utgangspunktet vare evig. Da objekter uten data har liten eller ingen vitenskapelig verdi, vil data knyttet til objektene i samlingen også oppbevares like lenge som objektene.

## *Datasubjektets rettigheter*

Personvernsforordningen pålegger behandlingsansvarlig å treffe egnede tiltak slik at datasubjektets rettigheter ivaretas (GDPR art. 12 til 14). Ved registrering av personopplysninger knyttet til tidligere innsamlede objekter, anses det som praktisk umulig å informere datasubjektene om registreringen og GDPR art. 14 nr. 5 bokstav b får anvendelse. Dette fordi museenes arkiver inneholder personopplysninger som strekker seg langt tilbake i tid og datasubjekt vil i mange tilfeller ikke være mulig å kontakte.

*Tilgang til dataene og dataportabilitet*

Datasubjektet har rett til innsyn i personopplysningene registrert om subjektet (GDPR art. 15) Museumsdataene som er tilknyttet objektet er i utgangspunktet offentlig tilgjengelig og kan søkes opp gjennom en rekke forskjellige nettportaler. Rådata fra museene er også fritt tilgjengelig for nedlastning (http://unimus.no/nedlasting/datasett/). Disse dataene er, så langt det er mulig, på internasjonale standardformater (som Dublin Core (http://dubincore.org/) og Darwin Core (http://rs.tdwg.org(dwc/)).

Personopplysninger som ikke ligger fritt på nettet (for eksempel fødselsdato), skal museene via søk fra basen gjøre tilgjengelig uten opphold. Det vurderes slik at dette er en enkel sak å utføre rent teknisk.

Rett til dataportabilitet (GDPR art. 20 nr.1) kommer ikke til anvendelse da personopplysningene er samlet inn for å «*utføre en oppgave i allmenhetens interesse*» (GDPR art. 20 nr.3).

*Feilretting og Sletting*

Datasubjektene har også rett til korrigering og sletting av personopplysninger (GDPR art. 16, 17 og 19). Men siden formålet med behandling av personopplysninger er i «allmenhetens interesse» og for «vitenskapelig eller historisk formål» så begrenser dette data-subjektets rettigheter (GDPR art. 16, 17 bokstav b og d, og 19). Gjenstander i museets samlinger har liten eller ingen verdi uten proveniens eller innsamlingskontekst (hvem, hvor og når), derfor vurderes det dithen at behandlingsansvarlig kan nekte sletting av personopplysninger (GDPR art. 17 (3) b og d).

*Rett til å protestere og begrense behandling*

Man har rett til å protestere og begrense behandling (GDPR art. 18, 19 og 21). Retten vil særlig gjøre seg gjeldende hvis det er uriktige opplysninger registret om personen (GDPR art 18 nr. 1 bokstav a).

Behandlingsansvarlig har plikt til å underrette datasubjektene om korrigering eller sletting av personopplysninger (GDPR art. 19). Vi anser at denne plikten bortfaller for museene da dette vil innebære en uforholdsmessig stor innsats da kontakt informasjon til datasubjektene ikke lagres i systemet. Innsigelsesrett nevnt bort-faller da behandlingen er «*nødvendig for å utføre en oppgave i allmennhetens interesse*» (GDPR art. 21 nr. 6). Det vurderes slik at dette vil gjelde alle registreringer av person-opplysninger.

Museene må opprette retningslinjer for intern databehandling da museene er behandlingsansvarlig. UiO er gjennom USIT databehandler og også behandlingsansvarlig for museene knyttet til UiO; Kulturhistorisk museum og Naturhistorisk museum. For de museene som ikke er en del av UiO (og dermed USIT) må det opprettes en databehandlingsavtale med USIT (GDPR art. 28 nr. 1 og nr.2).

*Internasjonal overføring*

**A.** gjennomføre sikkerhetstiltak ved internasjonal overføring (GDPR kap.V) er ikke aktuelt for MUSIT databasene, da dette i utgangspunktet ikke gjøres. Men det i de tilfeller da museene bruker innskrivningssentraler ut utlandet (f.eks. Alembo) kommer dette til anvendelse og museene må inngå EUs standard personvernbestemmelser (Standard Contractual Clauses) med dem.

*Forhåndskonsultering*

Det er ikke aktuelt med forhåndskonsultering (GDPR art. 36) da dataene ikke er «av særlige kategorier av opplysninger» (GDPR art. 9 nr. 1) eller av personopplysninger om straffedommer og straffbare forhold» (GDPR art. 10). Det forutsettes at eventuelle data i disse kategoriene slettes i MUSIT-basene.

## *Risiko*

Data som lagres om datasubjektene er navn, fødselsdato og opplysninger om hvor de har vært til et bestemt tidspunkt. Det lagres ikke data av «særlige kategorier av opplysninger» (GDPR art. 9 nr.1) med unntak av TopArk (se overfor) og mengde data om hvert subjekt er relativt begrenset. Derfor kan man i utgangspunktet anta at konsekvensene av en uønsket hendelse er liten sett fra datasubjektets side. Men det meste av dataene er fritt tilgjengelig og kan settes sammen med andre datasett og dermed få et bilde av personens aktiviteter. For eksempel kan Google indeksere dataene og knytte disse opp til andre data de allerede har om vedkommende.

Innsamlinger gjøres ofte sammen med andre personer, enten ved at de samler inn objektet sammen eller at man samler forskjellige objekter på samme geografiske lokalitet på samme tid. Dette kan for eksempel gjøres ved at man knytter objekt-data fra en person med observasjonsdata som Artsobservasjoner (www.artsobservasjoner.no) og da se hvem som har vært sammen. En annen risiko er at data om hvem som er saksbehandler og hva vedkommende har utført kan komme på avveie.

*Følger av uønskede hendelser*

Uønskede hendelser vil være tilgang til de personopplysningene vi ikke vil dele fritt; dette er fødselsdato, fødselsted, lenker til andre kilder om informasjon om de registrerte, samt historikk over saksbehandlings hendelser. Følgene av dette må i utgangspunktet anses som lite alvorlige. Unntaket kan være at kjennskap til personers fødselsdato kan lede til identitetstyverier og dette er svært alvorlig. Integritetsbrudd, tilgangsbrudd og/eller sletting/tap av data vil i denne sammenheng være endring/sletting av navn, fødselsdato og/eller hvilke objekter som er registret samlet inn av datasubjektet. Dette vil ha små konsekvenser for registerets rettigheter og friheter.

Datasikkerheten ligger under USIT som driver med kontinuerlig overvåking mot hacking og har et meget strengt sikkerhetsregime. Tilgangskontrollen styres via Feide og dataportalen, som er anbefalte nasjonale standarder (https://www.feide.no/om-feide). Det vurderes dithen at den IT tekniske sikkerheten er godt ivaretatt.

*Skadebegrensende tiltak*

Flere viktigste skadebegrensende tiltak har blitt gjennomført i arbeidet med å lage et nytt IT-system, dette er en nøye vurdering og en reduksjon av antallet/typene opplysninger som registreres om datasubjektene (GDPR art. 35 nr. 7 bokstav d).

*Involvering av berørte parter*

Behandlingsansvarlig kan bli pålagt følgene; «Dersom det er relevant, skal den behandlingsansvarlige innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter» (GDPR art. 35 nr. 9). Det er ofte medlemmer fra en rekke frivillige organisasjoner som samler inn og leverer materiale til museene. Disse kan kontaktes for å få synspunkter på behandlingen av data.

UiO, som er vertskap for MUSIT, har et personvernombud som har blitt kontaktet i forbindelse med utviklingen av nytt IT-system som oppfølging av GDPR (art. 35 nr.2). Totalt sett anses risiko for å være små/under kontroll, og personverns-konsekvensene som relativt små ved eventuelle brudd.

**Risikoanalyse**

Målet med risikoanalysen er å identifisere potensielt uønskede situasjoner, både for å være best mulig forberedt hvis de skulle inntreffe og for å kunne iverksette risikoforebyggende tiltak. Under er en tabell som viser usikkerhetene med en vurdering av sannsynlighet og konsekvens. Sannsynlighet multiplisert med konsekvens vil gi en risikofaktor som brukes til en rangering av tiltak og fokusområder. Konsekvenser rangeres fra «1 - ubetydelig», «2 - liten», «3 - moderat», «4- alvorlig» og «5 -veldig alvorlig». Sannsynlighet rangeres fra «1-veldig lav», «2-lav», «3-moderat», «4-høy» og «5-veldig høy».

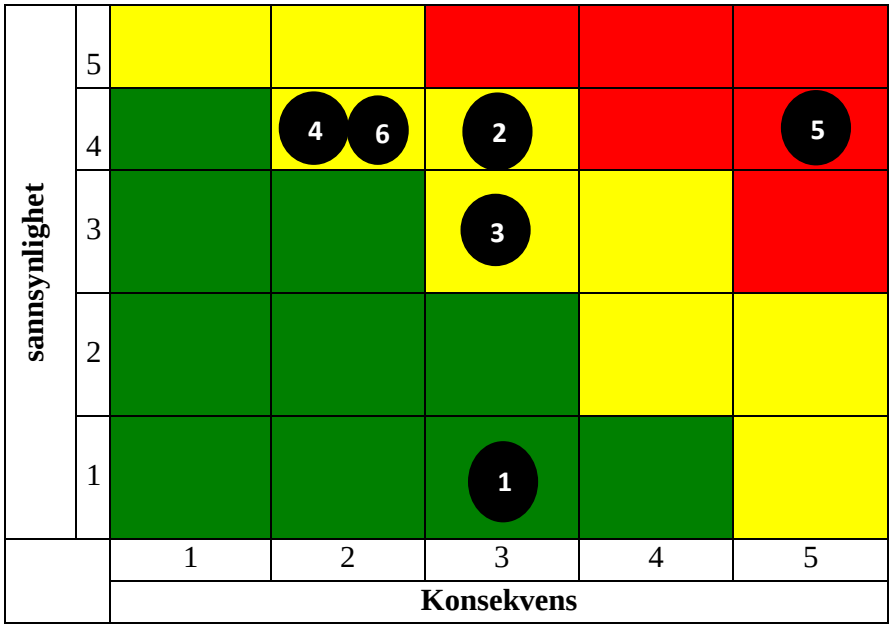
(S = sannsynlighet, K = konsekvens, R = risiko, R = S x K)

DBK= databasekoordinatorene, KG-koordineringsgruppene

| Nr | Usikkerhet | Beskrivelse av konsekvens | S | K | R | Forslag til risikoreduserende tiltak | Tiltaks-ansvarlig |
|---|---|---|---|---|---|---|---|
| 1. | Forankring av MUSITs GDPR-plan i ledelse ved museene og MUSITs styre. | Utfordringen er at museene ikke har egen tiltak for å møte og implementere universitetenes GDPR beslutninger. | 1 | 3 | 4 | Presentere MUSITs GDPR-plan til MUSITs styre og ledelse ved museene.<br><br>Etterspørre samarbeid med personvernombuds-representanter hos universitetene og museene knyttet til lokal GDPR-oppfølging. | MUSIT - daglig leder<br><br>GDPR ansvarlig ved museene |
| 2. | Kartlegging av personopplysning som er lagret i tilknytning til MUSIT-basene.<br><br>Enkelte har skrevet inn personopplysning i feil felter og lagret personopplysning | Det er lagret personopplysninger i databasen som er av særlig kategori, eller at personopplysninger kan eksponeres da de er skrevet inn i felter som deles med andre aktører. | 4 | 3 | 12 | Opplæring i innføring av personopplysninger i MUSIT-basene.<br><br>Kjøre regelmessige tekniske undersøkelse/søk i de aktuelle feltene for personopplysninger og informere database-koordinatorene ved museene. | Databaseko ordinator ved museene<br><br>USIT |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | som vedlegg til poster i MUSIT-databasen. | | | | | | |
| 3. | Karlegging av aktører og roller i utarbeidelse av databehandler-avtaler mellom USIT, museene, og andre. | Uklarhet om hvilken rolle en aktør har, og hvem som er ansvarlig for å få skrevet databehandleravtale med alle aktuelle partnere. | 3 | 3 | 9 | Gjennomgå eventuelle eksisterende databehandleravtaler og revidere dem. Hvis det ikke finnes en avtale utarbeide en databehandleravtale.<br><br>MUSIT ber USIT om å inngå databehandleravtale med hvert universitet/museene for å få like avtaler. | USIT<br><br>GDPR ansvarlig ved museene |
| 4. | Informasjon om personopplysninger av særlig kategori for TopArk-applikasjon, dets omfang og sikring. | Ved lagring av informasjon av særlig kategori i applikasjon for TopArk kan medføre til at uvedkommende får innsyn. | 4 | 2 | 8 | Ber de museene som har opplysninger av særlig kategori lagret i TopArk-applikasjon om å flytte / slette opplysning.<br><br>Musene tar en gjennomgang av rutiner for håndtering av personopplysning av særlig kategori i tilknytning til MUSIT. | USIT<br><br>Museene: databasekoordinator ved museene |
| 5. | Datafelter som deles med andre kan inneholde personopplysninger av særlig kategori. | Brudd på GDPR-regelverket. | 4 | 5 | 20 | Kartlegge hvilke datafelter som deles med andre som GBIF, Artsdatabanken, Norvegiana, og Europeana.<br><br>Sørge for at man begrenser delingen av personopplysninger til minimum, og at mottakerne oppdaterer sine oppføringer | USIT<br><br>MUSIT - daglig leder<br><br>Museene |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | hvis det blir endringer av personopplysningene. | |
| 6. | Undersøke om MUSIT-basene tilfredsstiller GDPR i forhold til logging. Lagres slike data for lenge? Logg er først registrert og siste endret. Men spesifikke hendelser er ment for å bevares. | Eventuelt brudd på GDPR art. 14 nr. 4 bokstav b. | 4 | 2 | 8 | Kartlegge hva som logges og gjennomføre en gjennomgang av disse postene med henblikk på GDPR art. 14 nr. 4 bokstav b.<br><br>Hvis nødvendig å igangsette tiltak. | USIT<br><br>MUSIT-daglig leder |



## *Handlingsplan med prioriteringer for å sikre samsvar med GDPR*

Handlingsplanen for å følge opp GDPR med tiltak er delt i ulike tema for å se sammenheng mellom like tiltak, og i prioriterte rekkefølge i hvert tema. Flere av tiltakene kan gjennomføres samtidig, noen tiltak er avhengig av at andre er blitt gjennomført først.

| A | DATABEHANDLER (AVTALE) | FRIST | ANSVARLIG |
|---|---|---|---|
| 1 | **Personvernombudet kontaktes**<br><br>Personvernombudet kontaktes for å gi råd i GDPR-prosessen, GDPR-plan og databehandleravtale GDPR art. 35 nr. 2.<br><br>Datatilsynets veileder – Personvernombudsordningen<br><br>https://www.datatilsynet.no/regelverk-og-skjema/veiledere/personvernombudsordningen/ | Høsten 2018 | GDPR ansvarlig ved museene |
| 2 | **Kartlegging av hvem som er databehandlere og behandlingsansvarlig**<br><br>Det må avklares hvem som er databehandlere og hvem som er behandlingsansvarlig (GDPR art 4 (7) og (8), 24, 28). I denne sammenheng må man ta for seg aktørene som via dataportaler deler museenes data på internett (GBIF osv.) (GDPR generelle best. 101). | Gjennomfør høste 2018 | MUSIT- Produkteier og daglig leder<br><br>USIT |
| 3 | **Kartlegging av eksterne aktører som mottar personopplysninger** Avklare om det trenges databehandleravtaler mellom | Høsten 2018 | MUSIT-daglig leder |

| | | | |
|---|---|---|---|
| | museene og eksterne aktører. GDPR art. 4 nr. 9. | | USIT |
| 4 | **Databehandleravtale mellom museene og USIT** Basert på kartlegging i oppgave 2 opprette databehandleravtaler (GDPR art. 28 nr. 3).<br><br>UiOs maler for databehandleravtaler blir brukt. | Høsten 2018 | GDPR ansvarlig ved museene<br><br>USIT |
| **B** | **KARTLEGGING** | | |
| 1 | **Karlegging av personopplysninger som lagres.**<br><br>Kartlegging bør inneholde: **a)** omfang, antall involverte personer**, b)** kategorier av personopplysninger, sensitive, ikke sensitive (GDPR art. 8, 9 og 10), **c)** hvilke personopplysninger deles med eksterne dataportaler. | | USIT<br><br>Museene: databasekoordinator ved museene |
| 2 | **Kartlegge hva som systemet automatisk logger av personopplysninger og hvor lang tid dette lagres.**<br><br>På bakgrunn av kartlegging av poster som logges vurderes nødvendige tiltak (GDPR art. 14 nr. 5 bokstav b). | Oktober 2018 | USIT |
| **C** | **RUTINER OG OPPLÆRING** | | |

| | | | |
|---|---|---|---|
| 1 | **Rutiner for behandling av personopplysninger i MUSIT-basene**<br>Det utarbeides retningslinjer for behandling og innlegging av person-opplysninger i MUSIT-basene (GDPR art. 5 og art. 24 nr. 1). | Høsten 2018 | Museene: databasekoordinator ved museene |
| 2 | **Opplæring av saksbehandlere i innføring av personopplysninger i MUSIT-basene**<br><br>Det gjennomføres opplæring i hva de ulike persondatafeltene i MUSIT-basene skal inneholde og ikke, spesielt i forhold til GDPR. Personvernombud ved museene kontaktes for å bistå. | November 2018 | Museene: databasekoordinator ved museene |
| **D** | **MOTTAK AV ULIKE MATERIALE TIL MUSEENE** | | |
| 1 | **Utarbeidelse av felles rutiner for mottak av potensielle museumsobjekter og donasjonskort**<br><br>Gjennomføres i forbindelse med Felles kvalitetssystem for samlingsforvaltningen prosjektet (FKS). Sørge for at alle som leverer materiale til museene godtar betingelser ved overlevering av materiale og at de informeres om at det lagres personopplysninger knyttet til avlevert materiale og rettigheter de har i den forbindelse med blant annet et informasjonskort/donasjonskort. GDPR art. 6 nr. 1 e. | | Museene |

| | | | |
|---|---|---|---|
| 2 | **Brev til organisasjoner om lagring av personopplysninger**<br><br>Brev sendes til ulike organisasjoner, hvis medlemmer leverer materiale til museene, med informasjon om museenes GDPR-tiltak. GDPR art. 6 nr. 1 e. | | Museene |
| **E** | **UTVIKLING AV NYTT IT-SYSTEM** | | |
| | **Videreutvikling av personmodul**<br><br>Sørge for at krav til innebygd personvern (GDPR art. 25) blir fulgt opp under utviklingen av nytt IT-system i samarbeid med personvernombudet ved UiO. | November 2018 | USIT<br><br>MUSIT- produkteier og daglig leder |
| | **Fjerning/sletting personopplysninger av særlig kategori**<br><br>Det antas at to museer har lagret personopplysninger av særlig kategori (GDPR art. 9 og art. 10). Selv om disse opplysningene er skjermet for innsyn i samsvar med Arkivloven (kapittel II. Offentlige arkiv. § 5), så skal de slettes eller flyttes informasjonen til et annet system. | Januar 2019 | Museene: databasekoordinator ved museene |
| | **Dataportabilitet, teste eksportfunksjonalitet**<br><br>Museene skal på forespørsel gjøre personopplysninger tilgjengelig til den registrerte (GDPR art. 20 nr. 1). Det gjennomføres en enkel testeksport i forbindelse med utviklingen av nytt IT-system for å teste at dette er mulig. | Høsten 2018 | USIT |

| | | | |
|---|---|---|---|
| | | | |
| | **Gjennomføre en ROS-analyse; vurdere datasikkerhet – datatekniske risikovurderinger**<br><br>Vurdere sikkerheten for datasubjektene med utgangspunkt i ROS-analysen. Forsikre at den tekniske sikkerhet omkring behandling av personopplysninger er i tråd med regelverket (GDPR art. 32). Det må eventuelt utarbeides tiltak i henhold til GDPR art. 24.<br><br>Det bli utført en ROS-analyse i januar 2017, denne må oppdateres i henhold til nytt regelverk. Som tidligere vil en ROS-analyse gjennomføres med bistand fra USITs sikkerhetssjef og en av USITs jurister. | Høsten 2018 | USIT<br><br>MUSIT- daglig leder |
| **F** | **DATADELINGSRUTINER** | | |
| | **Kartlegge hvilke nåværende datafelter som deles med andre**<br><br>Sørge for at man begrenser delingen av personopplysninger til minimum, og sørge for at mottakerne oppdaterer sine oppføringer hvis det blir endringer av personopplysningene (GDPR art. 16). | Høsten 2018 | USIT<br><br>MUSIT- daglig leder<br><br>Museene |
| **G** | **INFORMASJON** | | |
| | **Lage kommunikasjonsplan**<br><br>Det utarbeides en kommunikasjonsplan som sørger for informasjonsflyt og forankring av GDPR. | Oktober 2018 | MUSIT- daglig leder |

| | | | |
|---|---|---|---|
| | **Oppdatere MUSITs Wiki**<br><br>MUSITs Wiki skal være oppdaterte og inneholde relevant informasjon i tilknytning til MUSITs GDPR-arbeid, veiledninger og brukermanualer for behandling av personopplysninger i MUSIT-basene. | | MUSIT - daglig leder |

## *Litteratur og referanser*

Article 29 data protection working party, “Guidelines on Data Protection Officers (‘DPOs’) (WP 243rev.01), 30.10.2017.

Article 29 data protection working party, “Opinion on open data and public sector information (‘PSI’) reuse” (WP 207), 05.06.2016.

Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines" (WP 148) 04.04.2008

Artskart fra Artsdatabanken, https://artskart.artsdatabanken.no

Askeladden fra Riksantikvaren, https://www.riksantikvaren.no/Veiledning/Data-og-tjenester/Askeladden

Datatilsynet (2017) Veileder – Virksomhetens ansvar etter nytt regelverk, 13.06.2017. https://www.datatilsynet.no/regelverk-og-skjema/veiledere/virksomhetens-ansvar-etter-nytt-regelverk/

Datatilsynets (2018) Veileder – Personvernombudsordningen, Sitert 2.6.2018. https://www.datatilsynet.no/regelverk-og-skjema/veiledere/personvernombudsordningen/

Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/

uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf

Forskrift 9. februar 1979 nr. 8785 om faglig ansvarsfordeling mv. etter kulturminneloven.

Global Biodiversity Information Facility (GBIF), https://www.gbif.org

International council of museum (ICOM). Standard and guidelines 31.05.2018.
http://icom.museum/professional-standards/standards-guidelines/

Johansen, D.I. (2012). Organisasjonsendringer og organisasjonsledelse. Fagbokforlaget, Bergen. 339 s.

Kommunal- og moderniseringsdepartementet (2017). «Retningslinjer ved
tilgjengeliggjøring av offentlige data. 27.01.2017»
(https://www.regjeringen.no/no/dokumenter/retningslinjer-ved-
tilgjengeliggjoring-av-offentlige-data/id2536870/ )

Kommunal- og moderniseringsdepartementet (2017). Digitaliseringsrundskrivet
(rundskriv H 7/17).
https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2569983/

Lov 1. april 2005 nr. 15 om universiteter og høyskoler (universitets- og høyskoleloven).

Lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

Lov 19. juni 2009 nr. 100 om forvaltning av naturens mangfold (naturmangfoldloven).

Lov 27. juni 2008 nr. 71 om planlegging og byggesaksbehandling (plan- og bygningsloven).

Lov 9. juni 1978 nr. 50 om kulturminner (kulturminneloven).

MUSITs Strategidokument 2018 – 2023,

https://wiki.uio.no/usit/musit/images/e/e2/Strategidokument_MUSIT_2018_20 23.pdf

Prop. 56 LS (2017–2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.

Stortingsmelding nr. 15 (2007-2008). Tingenes tale Universitetsmuseene.

https://www.regjeringen.no/no/dokumenter/stmeld-nr-15-2007-2008-id503590/se